Risk-based Decision-making Guidelines

Volume 2
Introduction to Risk-based Decision Making

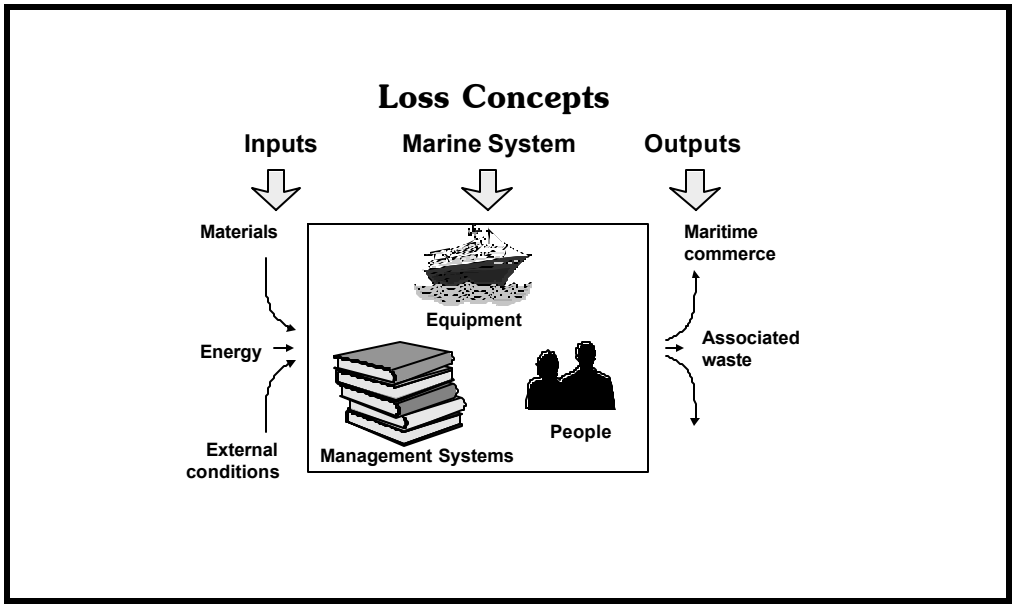
Basic Principles

Chapter 2 — Principles of Risk Assessment

Chapter Contents

This chapter provides an overview of basic risk assessment principles that play a key role in the risk-based decision-making process. This chapter is divided into six main topic areas:

Chapter Contents (cont.)



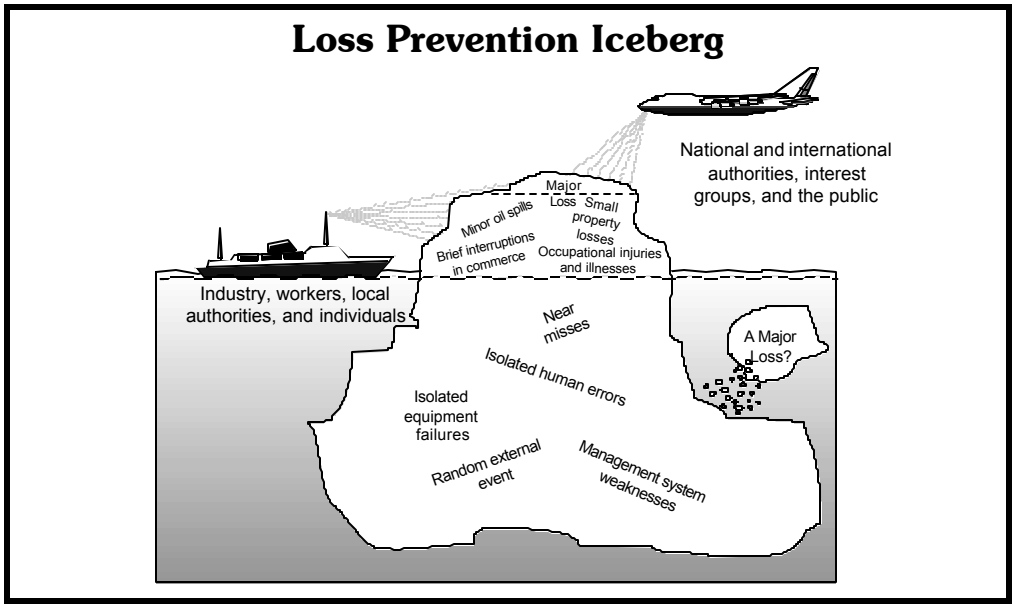
1.0 Loss Prevention Basics

Before you can learn to perform risk assessments, you need to understand how marine casualties occur and how they can be prevented.

What is a marine casualty?

A marine casualty is any event associated with a marine system (vessel, terminal, port, offshore platform, etc.) that leads to adverse effects on mariners, the public, property, commerce, or the environment. Marine casualties have the following characteristics:

- They are unplanned
- They involve human errors, equipment failures, or external events
- They have an impact on the economy, safety and health, or the environment
- They generally have underlying root causes that create error-likely situations for people and conditions leading to equipment failure
- They are frequently preceded by related events that can be detected and corrected
- They will always be possible, but can be effectively managed



1.1 Loss prevention iceberg

The loss prevention iceberg is an effective model for understanding marine casualties. The following sections describe how different groups view the events that make up the iceberg.

Iceberg structure

Top. The top of the iceberg is a small but critical area representing major losses. Major marine casualties are usually caused by many of the same problems that cause less severe, but more frequent, day-to-day problems.

Visible remainder. The visible remainder above the water is a significant area representing the day-to-day marine casualties that produce safety, environmental, or economic losses.

Shallow submerged. The shallow submerged area represents abnormal events that almost resulted in losses. Generally, these near misses largely outnumber actual day-to-day marine casualties and can be considered prior events leading to actual losses.

Deeper submerged. The deeper submerged area represents the many human errors, equipment failures, and external events that cause marine casualties and near misses.

Bottom. The bottom of the iceberg represents the underlying management system weaknesses that create the following:

- Error-likely situations for people
- Conditions leading to equipment failures
- Inadequate protections against external events

Different views of loss prevention

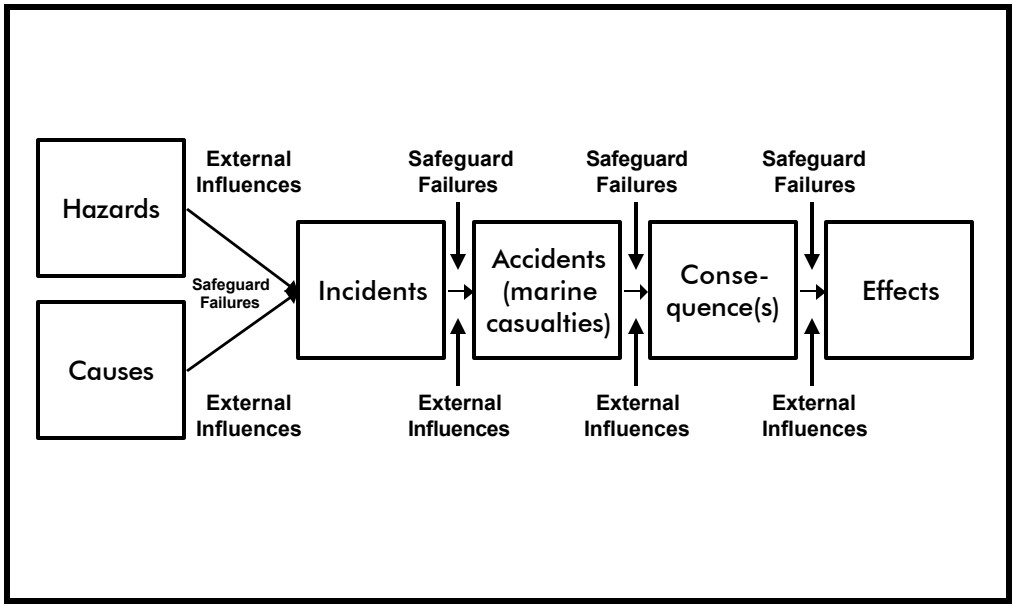
People see parts of the loss prevention iceberg differently.

- **National and international authorities, interest groups, and the public.** These people focus on the top of the iceberg to avoid major marine casualties, or large numbers of less severe casualties, that threaten the organization or lead to significant negative publicity. They leave less severe marine casualties and loss prevention management to others.
- **Industry, workers, local authorities, and individuals.** These people focus on the visible remainder of the iceberg to reduce routine marine casualties that impact productivity and cause management headaches. They pay attention to events that almost cause casualties (i.e., near misses), although they usually have trouble seeing these events. They have difficulty finding the time and resources to investigate and prevent the underlying problems.

Buoyancy principle as a guide for loss prevention

- Removing large portions of the iceberg above the water causes the iceberg to rise. Addressing only the visible events helps reduce the size of the iceberg, but it will rise and make other events (actual marine casualties) visible.
- Removing portions of the iceberg below the water causes the iceberg to sink. Addressing the underlying problems helps reduce the size of the iceberg and the number of visible events (actual marine casualties) above the water.

Remember, we cannot get rid of the entire iceberg. Even if there are no visible problems, danger still exists below the water. Major events can also break off from the iceberg without warning. However, our attention must certainly focus on identifying and correcting the underlying root causes of our loss exposures as represented by the portion of the iceberg below the waterline. We clearly cannot simply wait until types of marine casualties become visible, by actually causing loss, and then taking actions to prevent recurrence.



1.2 The accident sequence: Elements of a marine casualty

Marine casualties usually occur through a chain of events ending in one or more unwanted effects. This chain of events begins with *hazards* capable of causing casualties. If there are no hazards, there are no casualties. An equipment failure, human error, or external event is necessary for a hazard to cause an accident (i.e., a marine casualty). The Coast Guard refers to this *initiating event* as an *incident*. Sometimes one or more equipment failures, human errors, or external events must take place after the initial incident (i.e., the initiating event) for an accident to occur. An accident has at least one unwanted *consequence* with a measurable *effect*. This outcome is influenced throughout the chain of events by the presence of *safeguards* and their success or failure.

Causes are the underlying reasons why the initial incident occurs and safeguard failures allow the chain of events to progress. These are sometimes also called root causes of the accident. The following pages describe the chain of events in more detail.

Definitions of terms commonly used in risk assessment

Hazards — Situations, conditions, characteristics, or properties that create the possibility of unwanted consequences

Incidents or initiating events — Events in an accident sequence that begin a chain of events. This chain of events will result in one or more unwanted consequences with measurable effects unless planned safeguards interrupt the progression of the chain.

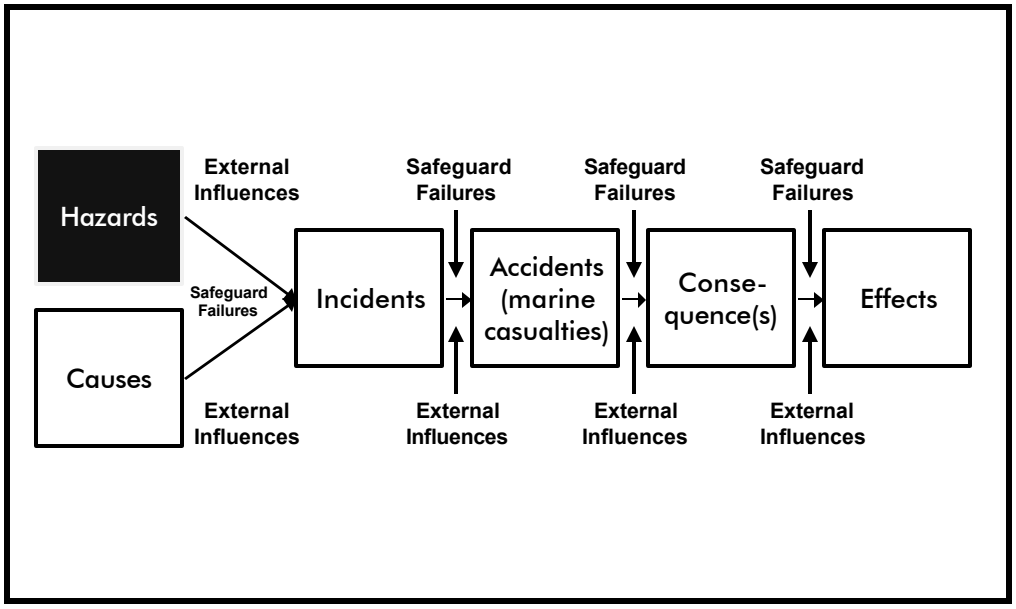
Accidents — Marine casualties such as a collision, grounding, allision, capsizing, sinking, or exposure of a mariner to a specific hazardous condition

Consequences — Unwanted events that can negatively affect subjects of interest. These include property damage or loss, mariner injury or illness, oil spill, loss of marine commerce, etc.

Effects — Measurable negative impacts on subjects of interest (i.e., the magnitudes of the consequences)

Safeguards — Planned protections that are intended to interrupt the progression of accident sequences at various points in accident chains of events. Safeguards can be applied as barriers at any or all of the transitions (i.e., arrows) in the accident sequence model. These planned protections may be physical devices, human interventions, or administrative policies.

Causes — Underlying reasons why the initial incident occurs and safeguards fail to interrupt the chain of events. The causes, sometimes called root causes, are typically weaknesses in management systems, which create error-likely situations for people and vulnerabilities in equipment.



1.2.1 Elements of a marine casualty: Hazards

The following sections describe the major categories of hazards likely to be encountered in traditional marine systems.

Combustible or flammable hazards. Combustible or flammable hazards exist when there is the potential for one or more materials to quickly react with air or some other oxidant, releasing energy in the form of heat and light.

Examples:

- Hydrocarbons and hydrocarbon derivatives (oil, LNG, LPG, etc.)
- Hydrogen
- Other gases (e.g., carbon monoxide)
- Finely powdered nonflammable materials
- Various metals (depending on the oxidizer)
- Wood products
- Cloth materials

Explosion hazards. Explosion hazards exist when there is the potential for one or more substances to release energy over a short period of time, creating a pressure wave that travels away from the source.

Examples:

- Many flammable materials
- Powders and dusts
- Nitrates
- Peroxides
- Highly reactive materials
- Strong oxidizers
- Cryogenic liquids
- Compressed or liquefied gases

Toxic hazards. Toxic hazards exist when there is the potential for one or more materials to cause biological damage to surrounding organisms by being absorbed through the skin, inhaled, eaten, or injected.

Examples:

- Chlorine or bromine
- Cleaning and maintenance fluids
- Contaminated food, water, and medical supplies

Asphyxiant hazards. Asphyxiant hazards exist when there is the potential for one or more materials to prevent organisms from breathing.

- **Simple asphyxiants.** Simple asphyxiants are usually nontoxic gases that replace the oxygen necessary to support life. Common simple asphyxiants are carbon dioxide and nitrogen.

- **Chemical asphyxiants.** Chemical asphyxiants are materials that stop organisms from using oxygen. Carbon monoxide is a chemical asphyxiant that prevents hemoglobin from carrying oxygen.

Corrosivity hazards. A corrosivity hazard exists when there is the potential for one or more materials to chemically burn body tissues, especially the skin and eyes, or to excessively erode or dissolve materials of construction or emergency response equipment.

Examples:

- Cleaning and maintenance fluids
- Battery acid
- Bleach

Chemical reactant hazards. A chemical reactant hazard exists when there is the potential for one or more materials to chemically combine, or to self-react, and produce unwanted consequences.

Examples:

- The side-by-side storage of reactive materials
- Reactive contaminants in materials

Thermal hazards. A thermal hazard exists when there is the potential for very hot or cold temperatures to produce unwanted consequences affecting people, materials, equipment, or work areas.

Examples:

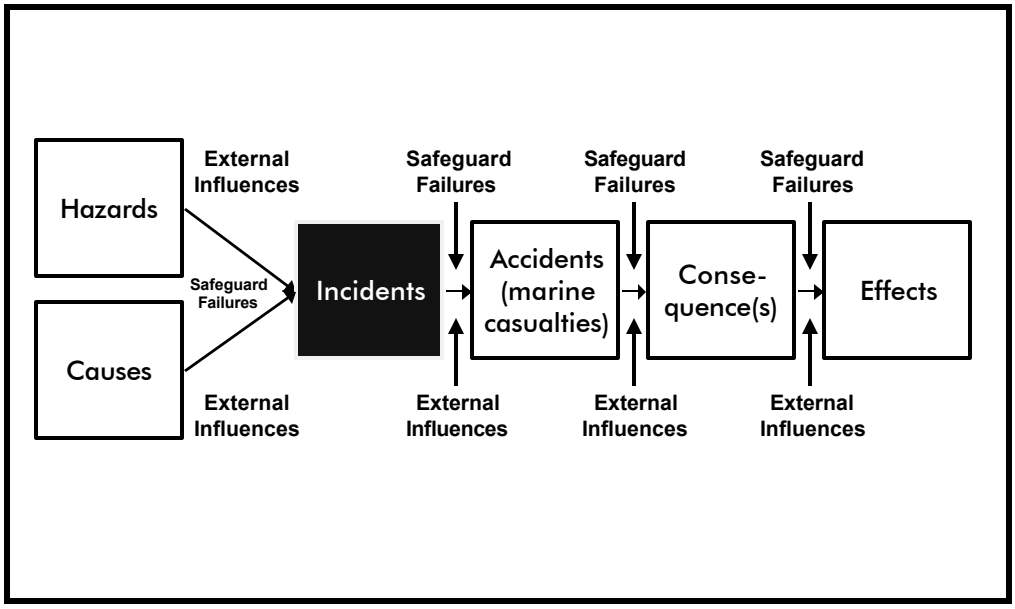
- Exposed or uninsulated high- or low-temperature equipment or materials
- Fires or explosions
- Chemical reactions
- Extreme ambient conditions and other equipment or operations in the area
- Phase changes
- Gas compression or expansion
- Friction

Potential energy hazards. Potential energy hazards exist when unwanted consequences can result from the following:

- High pressures other than explosions (e.g., normal operational pressures)
- Low pressures (e.g., vacuum conditions)
- Mass, gravity, or height (e.g., lifting operations)

Kinetic energy hazards. Kinetic energy hazards exist when unwanted consequences can result from motion of materials, equipment, or vehicles.

Electrical energy hazards. Electrical energy hazards exist when unwanted consequences can result from contact with, or failure of, manufactured or natural sources of electrical voltage or current. Examples include lightning, electrical charges, short circuits, stray currents, and loss of power sources.



1.2.2 Elements of a marine casualty: Incidents (initiating events)

Incidents are also known as initiating events. As defined by the Coast Guard, they start the actual chain of events leading to marine casualties. In some cases, this chain of events can be quite long, when many layers of protection exist against losses.

Incidents can be equipment failures, human errors, external influences, or any action or occurrence.

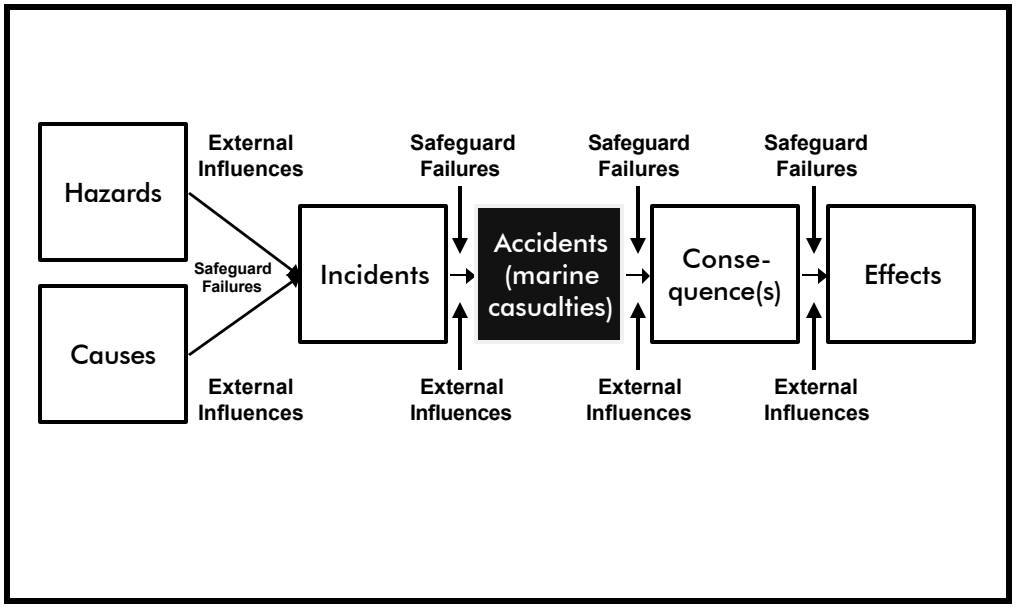
Examples:

- A rudder breaking
- An engineer incorrectly setting a control
- A fuel leak developing
- A rogue wave

Often, an initial incident challenges protective features that also must fail before an incident can become an accident. These special types of safeguards are call **demanded events.** Demanded events can be failed responses to initiating events by equipment or humans. Sometimes, other external events or conditions also influence the progress of an event chain and can be considered a demanded event.

Examples:

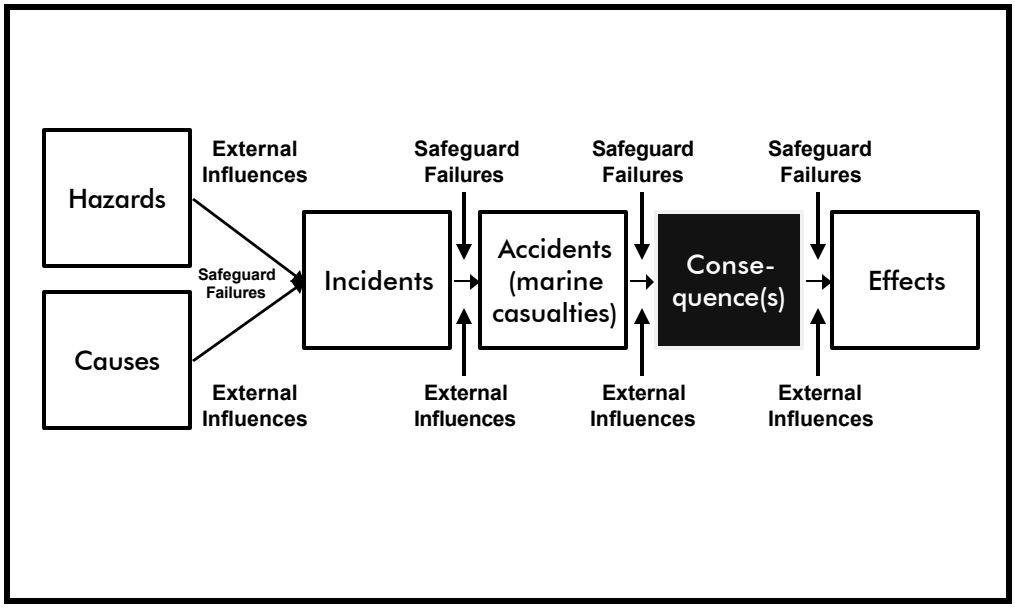
- Relief valve failing to act to reduce a pressure excursion
- Safety observer failing to interrupt an evolution to correct a safety problem



1.2.3 Elements of a marine casualty: Accidents (marine casualties)

The undesired marine casualties that are possible when a chain of events is completed can be classified in many ways. The following table provides an example of some marine casualties of interest.

Some Marine Casualties of Interest	
Capsizing	Drowning
Collision with another vessel	Person overboard
Allision	Spill of material
Collision with a floating object	Acute hazard exposure: workers
Grounding	Acute hazard exposure: public
Sinking	Nonconformance leading to loss of commerce
Fire or explosion	



1.2.4 Elements of a marine casualty: Consequences

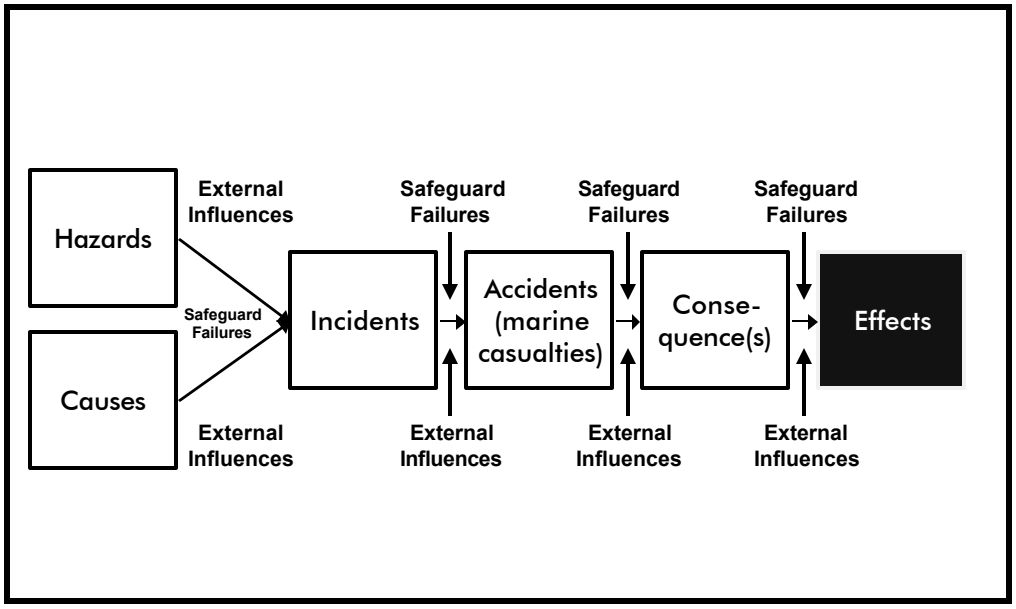
Marine casualties can result in different types of losses for various stakeholders. Some of these consequences include the following:

Mariner safety and health impacts (e.g., injuries or illnesses)

Public safety and health impacts (e.g., injuries or illnesses)

Economic impacts (property damage or loss of commerce)

Environmental impacts (releases of contaminants, such as oil or other hazardous materials)

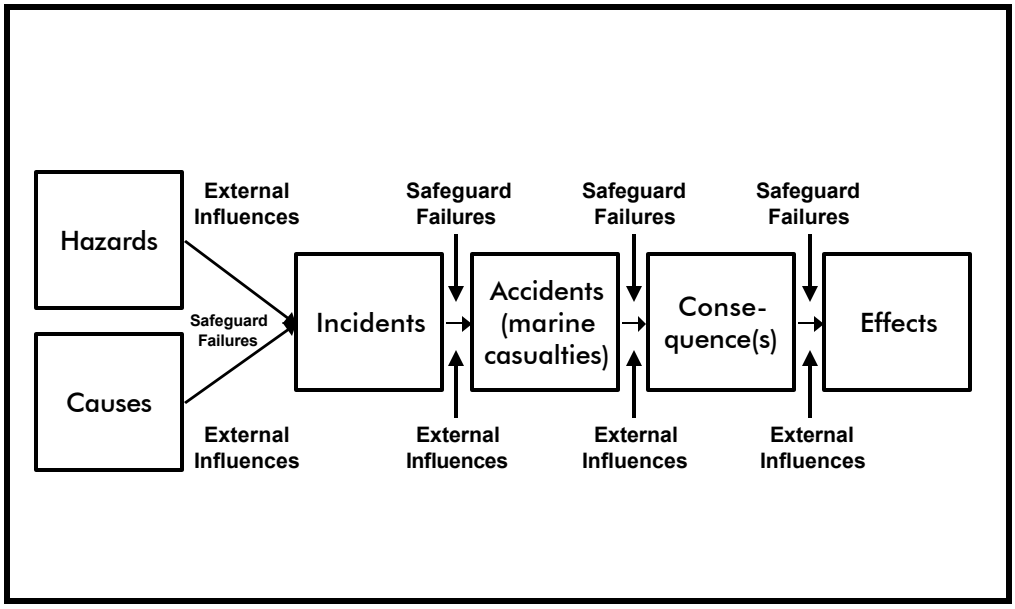


1.2.5 Elements of a marine casualty: Effects

The levels of effect related to consequences can be classified in many ways. The following table provides an example of how the Coast Guard has characterized levels of effect in at least one risk analysis.

Example Types of Effects*				
Severity	**Safety Impact**	**Environmental Impact**	**Economic Impact**	**Mission Impact**
Major (1)	One or more deaths or permanent disability	Releases that result in long-term disruption of the ecosystem or long-term exposure to chronic health risks	≥ $3M	≥ $3M
Moderate (2)	Injury that requires hospitalization or lost work days	Releases that result in short-term disruption of the ecosystem	≥$10K and <$3M	≥$10K and <$3M
Minor (3)	Injury that requires first aid	Pollution with minimal acute environmental or public health impact	≥ $100 and <$10K	≥ $100 and <$10K

* Losses in these categories result from both immediate and long-term effects (e.g., considering both acute and chronic effects when evaluating safety and health).

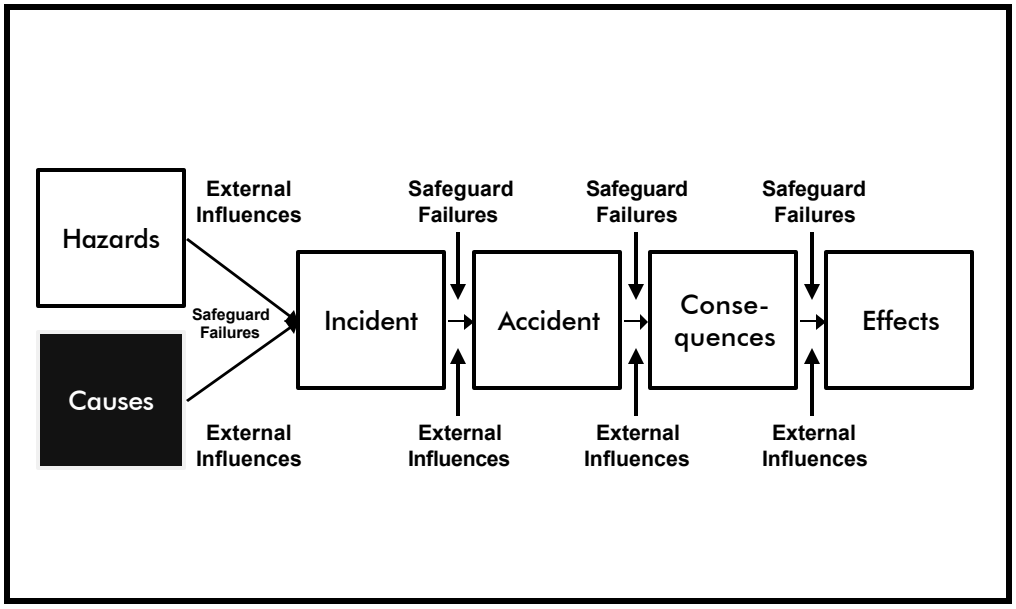


1.2.6 Elements of a marine casualty: Safeguards

Safeguards can be engineered systems, human monitoring and response, or administrative policies and programs for (1) reducing hazards, (2) preventing incidents, (3) interrupting chains of events before casualties occur, (4) reducing consequences, or (5) reducing effects. Safeguards, especially administrative safeguards, also help eliminate the underlying causes of the events in the accident chain.

Examples:

- Preventive maintenance for the steering system and relief valves
- Policy requiring a safety supervisor for all deck operations
- Personnel qualification programs for a key position
- Vessel classification
- Coast Guard inspections (dry-dock inspections)
- Coast Guard presence at port marine events



1.2.7 Elements of a marine casualty: Causes

The chain of events leading to an accident typically involves a series of human errors, equipment failures, and external influences. However, these are seldom the true causes of the accidents. Organizational issues, often referred to as management system weaknesses, are really the root causes of most accidents. Examples of these root causes include, but are certainly not limited to, the following:

For equipment failures:

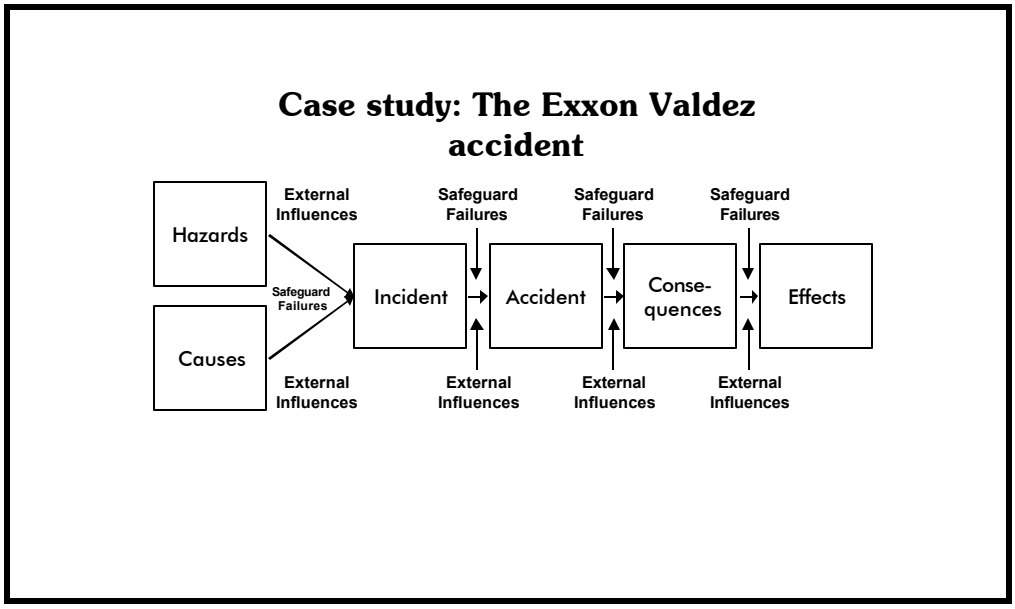
- Inappropriate design or application
- Lack of predictive or preventive maintenance
- Erroneous repairs
- Unrecognized or ill-advised equipment changes

For human errors:

- Wrong, confusing, or missing procedures
- Lack of, wrong, or incomplete training
- Poor human/system interfaces
- Poor work conditions
- Excessive workload
- Lack of or deficient communication systems or processes
- Lack of or deficient supervision
- Poor workplace culture and motivational issues

For external influences

- Failing to anticipate and protect against reasonably foreseeable external conditions such as poor weather



1.3 Case study: The Exxon Valdez accident

In 1989, a major oil spill occurred in Prince William Sound, Alaska, when the Exxon Valdez ran aground while leaving the Aleyeska Marine Terminal. The following sections describe the chain of events involved in this catastrophic loss.

Hazards

- Oil (environmental pollutant and toxin)
- Kinetic energy of vessel

Incident (initiating event)

- The captain ordered the helmsman to leave the shipping lanes to steer around icebergs

Accident

- Vessel ran aground

Consequences

- 600-foot hole ripped in the bottom of the tanker
- 240,000 barrels (10,000,000 gallons) of oil spilled, causing catastrophic damage to the local environment

Effects

- Major environmental damage, including many dead animals
  - 1,000+ otters
  - 35,000+ birds
- $1 billion+ in cleanup costs

Long-range impacts

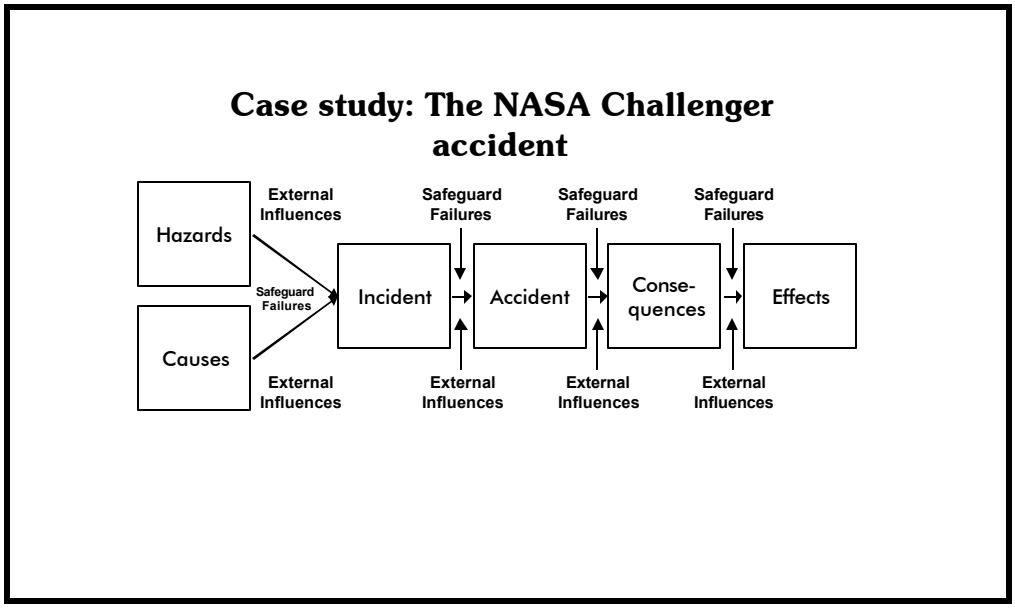
- Environmental damage to Prince William Sound
- Fishing fleet in area affected
- Increased public concern about transportation accidents, especially in ship traffic in Prince William Sound

Failed safeguards and external influences

- The captain left orders with the third mate to turn back into the shipping lanes at a certain point, and the captain then left the bridge
- The third mate failed to order the new helmsman to turn back into the shipping lanes at the point prescribed by the captain
- Captain not on bridge
- Experienced mate not in charge of critical turn
- First cleanup team did not arrive until 14 hours after the spill
  - *dedicated* recovery barge had been in dry dock for repairs for the last 2 months
  - booms and skimmer equipment had to be located and loaded onto barge
  - once loaded, the barge was unloaded to transport pumps needed to transfer oil from the Exxon Valdez to another ship
- Dispersants to be used on spill
  - worldwide supply was not large enough for this size of spill
  - authorization to use dispersants was not given for 3 days
- Response was disorganized because of lack of planning; 48 hours after the spill, only 3,000 of 240,000 barrels of oil were recovered

Safeguards not provided

- Double hull tanker
  - double hull may not have prevented the spill, but could have reduced the consequences and effects
- Effective Coast Guard monitoring capability



1.4 Case study: The NASA Challenger accident

In 1986, the space shuttle Challenger exploded 73 seconds after lift-off from the Kennedy Space Center in Florida. The following sections describe the chain of events involved in this catastrophic loss.

Hazard

- Fire and explosion hazards of fuels (liquid hydrogen and liquid oxygen)

Incident (initiating event)

- Lift-off of a shuttle when the ambient temperature was low

Accident

- Flight 51-L explodes 73 seconds after lift-off

Consequences

- Loss of seven astronauts
- Loss of a multi-billion-dollar shuttle

Effects

- Seven fatalities
- Multi-billion dollar economic loss
- Major impact on shuttle program

Long-range impacts

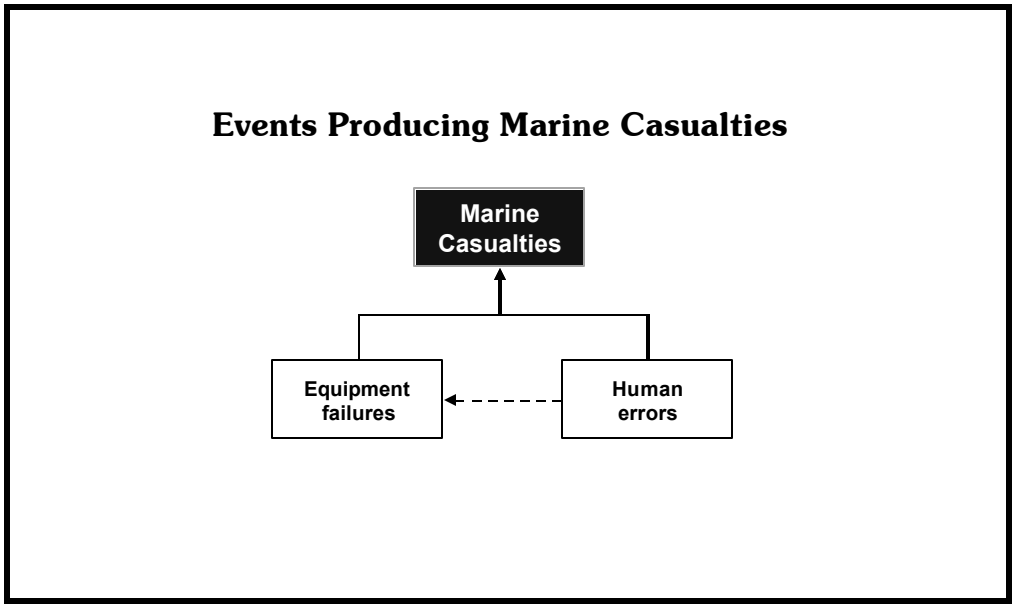
- Suspension of the shuttle program for almost three years
- Safety culture of NASA considered suspect

Failed safeguards and external influences

- Solid rocket motor rubber O-ring failed to seal properly because of its reduced pliability from sitting at a low temperature prior to launch
- Heavy wind shear during the last 45 seconds of the flight caused higher than normal bending of the joints of the solid rocket motor sealed by the rubber O-ring
- High-pressure hot exhaust gases from the solid rocket motor eroded through the cold rubber O-ring (aided by the higher-than-normal bending of the joint) and contacted the external fuel tank
- Ineffective management assessment of identified issues
  - temperature effects on O-rings not well understood by launch safety personnel
  - no definite operating envelope was set for O-rings
  - design specification did not include a temperature range
- Prior evidence of O-ring problems was not viewed as a problem
  - O-ring damage was observed on 15 of 25 missions
  - eventually, O-ring damage was viewed as acceptable

Safeguards not provided

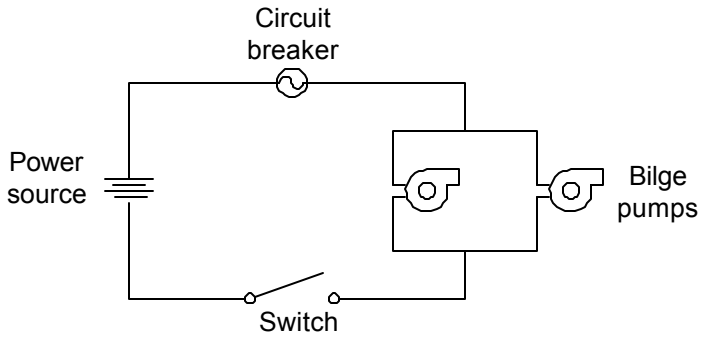
- Effective O-ring design
- Timely communication of temperature limit for O-rings in this service



2.0 Events Producing Marine Casualties

A marine casualty is caused by a combination of one or more equipment failures or human errors.

Example



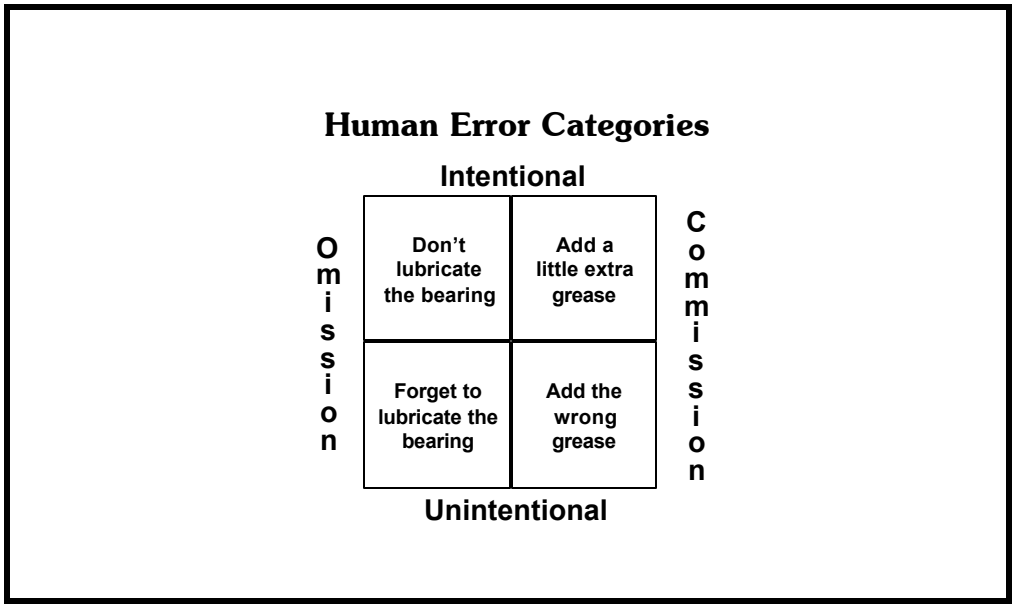
Assume a bilge pumping system has a single power supply and two pumps in parallel. The entire circuit is protected by a single breaker and controlled by a single switch. The following are events contributing to a lack of bilge pumping:

- Power supply fails off
- Wiring fails
- Circuit breaker fails open
- Switch fails open
- Operator unintentionally opens switch
- Pump #1 fails off; pump #2 fails off

The keys to preventing accidents are (1) understanding the combinations of events leading to an accident and (2) knowing how to make the equipment failures and human errors less likely.

There is an entire science dedicated to forensic analysis of equipment failures, which is more than could be addressed in these *Guidelines*. However, a good technical knowledge of equipment failure mechanisms is often important for identifying and managing risks. Straightforward texts such as Donald Wulpi's *Understanding How Components Fail* and ASM International's *Principles of Failure Analysis* are good references for developing a more in-depth knowledge in this area.

Often overlooked is the importance of human error prevention in risk management. In fact, human error is also the underlying cause of most equipment failures. After all, who designs, builds, manufactures, installs, operates, and maintains the equipment? People! Because of the importance of human error in marine risk management, section 3 of this chapter explores human error in more detail. Of course, there is also a whole field of study dedicated to preventing human errors and improving human performance.



3.0 What is Human Error?

The term "human error" refers to human actions or inactions outside the tolerances established by a system, even if no immediate consequences occur. Systems within every industry are almost always subject to failure as a result of human error.

Human error includes the following:

- Personnel not following procedures or neglecting routine duties
- Improper or inadequate training of workers or crew
- Errors in writing operating instructions
- Equipment or system design, construction, or installation errors
- Improper or inadequate inspection, testing, or repair of equipment
- Lack of management oversight

Human error excludes *deliberate actions performed with harmful intentions (i.e., sabotage).*

A human error is typically characterized by the following descriptions:

Error of omission. Failure to perform a task or step

Error of commission. Performing a task or step incorrectly, as in the following:

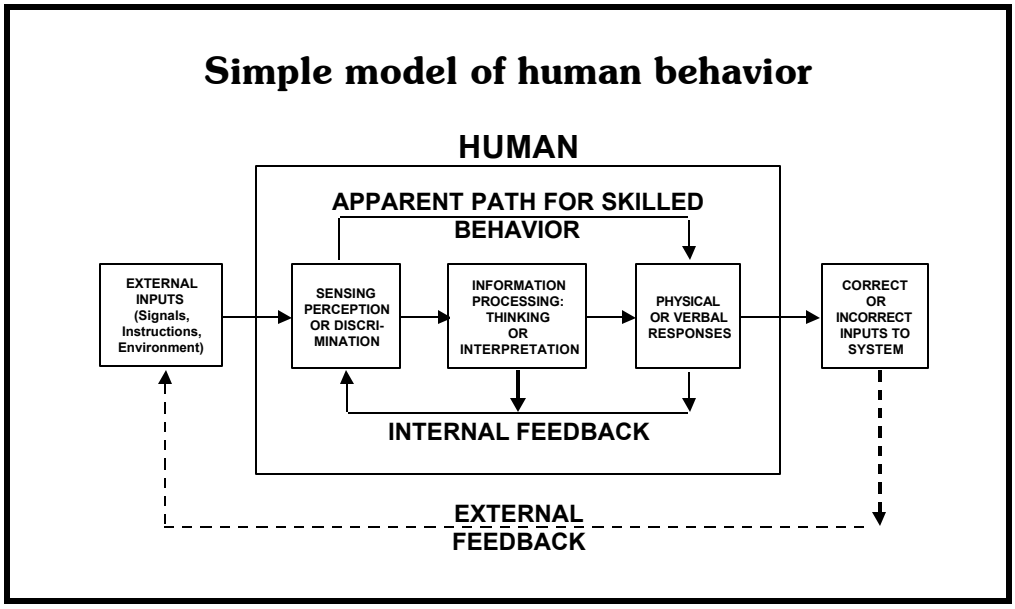
- Selection error
  - selects wrong display or device
  - mispositions device
  - issues wrong command or information
  - too slow
- Extraneous act
- Sequence error
  - too soon
  - too late
- Time error
  - too long
  - too short
- Quantitative error
  - too little
  - too much
  - too fast

Unintentional error. An action committed or omitted *accidentally*, with no prior thought

Intentional errors. An intentional error does *not* include sabotage. The difference is in the *motive*. This error includes the following:

- An action committed or omitted deliberately, because of a perception that there is a better or equally effective way to perform the task or step. This is often a *shortcut* that may not be recognized as a mistake until other conditions arise that result in a noticeable problem.
- An action committed or omitted because the worker *misdiagnosed* the system's problem or need. At best, such an action delays the correct response; at worst, it compounds the problem.

For more information on human error in the Coast Guard, see the document entitled "Human Error and Marine Safety" in the General Resources Directory in Volume 4.



3.1 Simple model of human behavior

Human interaction with a system can be modeled as a component with three distinct functions. The rest of the system continuously provides information that enters the human through one of our five senses.

1. **Sensor, perception, or discrimination.** The brain filters out most external inputs as irrelevant information. The first task of the human "component" is to recognize important information and discriminate it from background noise.
2. **Information processing: thinking or interpretation.** The human must then process the input to determine its meaning and to select an appropriate response. When people practice the same response to a given input, they eventually appear to bypass this function (i.e., the apparent path for skilled behavior). This is when actions become second nature and explains why simply retraining and improving procedures often does not improve human performance.
3. **Physical or verbal responses.** Finally, the human physically responds based on the perceived or processed information. Lack of action is also a response.

The response in turn provides new inputs to the human who can sense his or her own actions (internal feedback) and sense how the system is responding (external feedback). Well-designed systems react perceptibly to the new input and provide feedback to the human by altering the external inputs.

Application of the model of human behavior

Suppose a ferry is transitioning across a bay and a small craft begins to cross its path. The crew of the ferry must alter course to avoid a collision.

External inputs

The presence of the small craft should provide an input to the ferry's crew. Other inputs might be radar contacts, radio messages, horns, etc. Without their other inputs, the crew might not recognize the small craft in their course soon enough. Diverse, reliable, and recognizable inputs are important for good human performance.

Sensing, perception, and discrimination

Even if the inputs exist, the crew must be able to recognize the inputs. Impaired visibility, distractions, too many messages or contacts, and various other situations can keep the crew from accurately sensing the key inputs.

Information processing

Once the crew recognizes that the small craft is crossing its path, it must decide what action to take. The proper response probably depends on many factors, such as other vessel traffic, weather and sea conditions, position in the bay, etc. In most cases, we would hope for a well-reasoned choice of what actions to take. However, if this happens often or if little time to react is available, the crew may largely omit this step, reacting by experience and instinct.

Physical or verbal responses

Next, the crew would take actions such as powering down the vessel, making an evasive maneuver, alerting the small craft to the danger, etc. As members of the crew take these actions, they will be able to sense their own actions and adjust the magnitude of the response.

Correct or incorrect inputs to systems

The crew's actions will cause the ferry to respond by slowing or turning. The response of the ferry, and possibly the small craft, will create a whole new set of inputs for the crew.

This process is continually occurring for all of us!

Results of error-likely situations

- **Lack of external input**
- **Failure to sense input**
- **Misinterpretation of input**
- **Inappropriate response**
- **Lack of feedback**

3.2 Results of error-likely situations

Error-likely situations can exist at any element of the human performance model. Examples of such deficiencies related to the example application in section 3.1 include the following:

Lack of external input such as signals or instructions. The person doesn't know that he or she should act because there is no signal provided to the user.

- Crew does not receive a radar contact warning because the radar is malfunctioning
- No traffic control system is in place to warn the crew
- The small craft does not have the proper navigation lights for nighttime operation

Failure to sense input. An input signal is provided but is not sensed because of information overload, insufficient discrimination, or poorly organized information.

- Weather conditions prevent the crew from seeing the small craft
- The crew is distracted with some other problem aboard the ferry
- Too much radio traffic or garbled messages confuse the crew
- The bridge of the ferry has a blind spot

Information presented to the user must be organized and prioritized. Important and urgent inputs must stand out from others.

Training and experience can increase the likelihood that appropriate signals are identified, but system design is the key to correcting these issues.

Misinterpretation of input. The input signal is clearly noted, but the meaning of the signal is misinterpreted.

- The crew believed that the vessels would pass without taking an action
- The crew mistakenly thought that the small craft was taking evasive action

Systems should provide unambiguous indications of their status and the required action. Training and experience can increase the probability of correct interpretations.

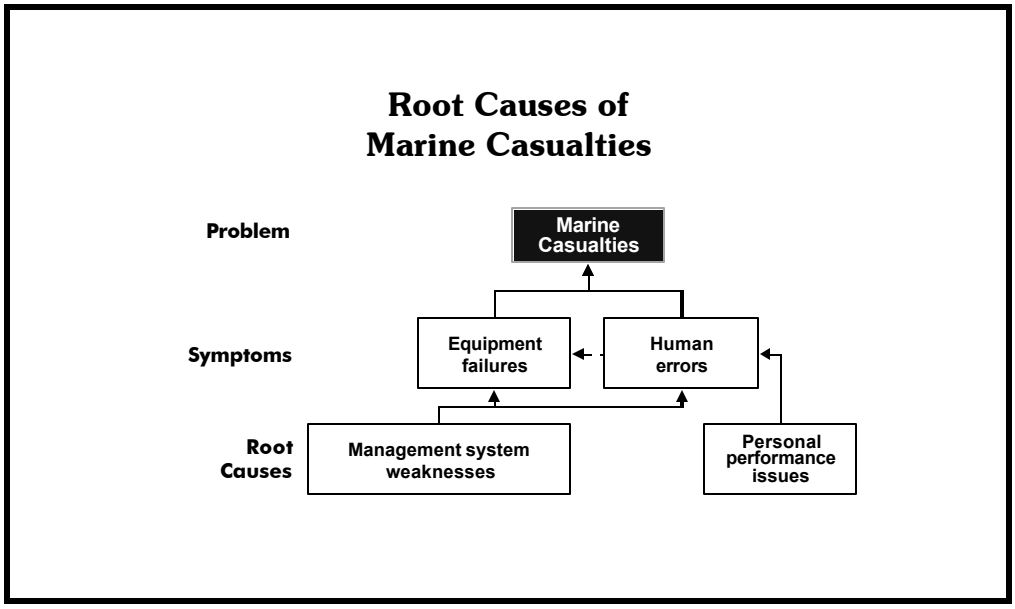
Inappropriate or insufficient physical or verbal response. The user knows what to do and how to do it, but he or she takes inappropriate action.

- The crew fails to maneuver the vessel appropriately
- The crew fails to alert the small craft
- The sea state or current makes the evasive maneuver ineffective

A system may require a high level of skill or physical strength to get an acceptable response. Examples of this fact are surgeons and athletes. Practicing the skill or better matching the person to the task can increase the likelihood of the appropriate response.

Lack of feedback. There is no indication that the user did the previous steps (sensing, interpreting, responding) correctly, or feedback is too vague or not timely.

- The small craft does not respond to warning messages or signals
- The ferry responds too slowly to control adjustments, and the crew does not have a chance to refine the adjustments



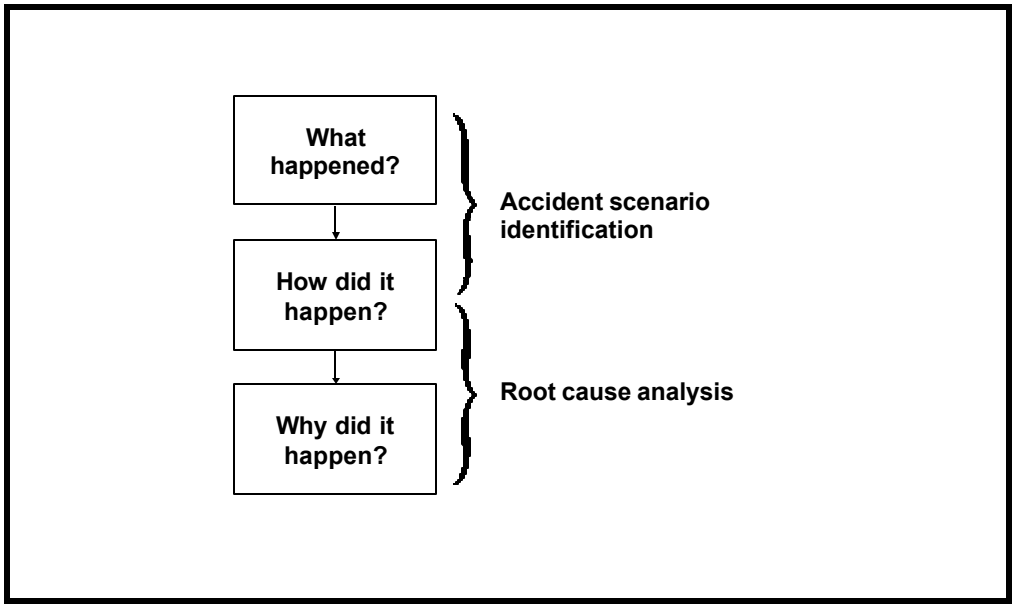
4.0 Introduction to Root Causes

Marine casualties are caused by combinations of equipment failure and human error. Sometimes the underlying causes result from personal performance errors; that is, all practical measures for preventing the errors had been tried. Humans will eventually make mistakes with even the most error-proofed systems. However, the underlying causes can usually be traced to weaknesses in an organization's management systems; that is, its programs and policies. These management system weaknesses lead to conditions for equipment failure and error-likely situations for individuals. These are the underlying root causes of most marine casualties and other unwanted situations, such as inspection deficiencies.

What is a root cause?

- Root causes are the most basic causes of an event that meet the following conditions:
  - they can be reasonably identified
  - management has the ability to fix or influence them
- Typically, root causes are the absence, neglect, or deficiencies of management systems that control human actions and equipment performance

For any event leading to a marine casualty, there may be more than one underlying root cause. It is not uncommon for a marine casualty to have many underlying root causes. If these root causes are not found and corrected, the underlying management system weaknesses will lead to marine casualties.



4.1 What is root cause analysis?

Root cause analysis provides a means to determine how and why something occurred. Understanding the accident scenario is not enough. Scenarios tell us what happened, not why it happened. Events in accident scenarios are generally only symptoms of underlying problems in the administrative controls that are supposed to keep those events from occurring. Understanding only the scenario addresses the outward symptoms, but not the underlying problems. More investigation of the underlying problems is needed to find and correct those that will contribute to future accidents. Root cause analysis provides a means to investigate underlying problems.

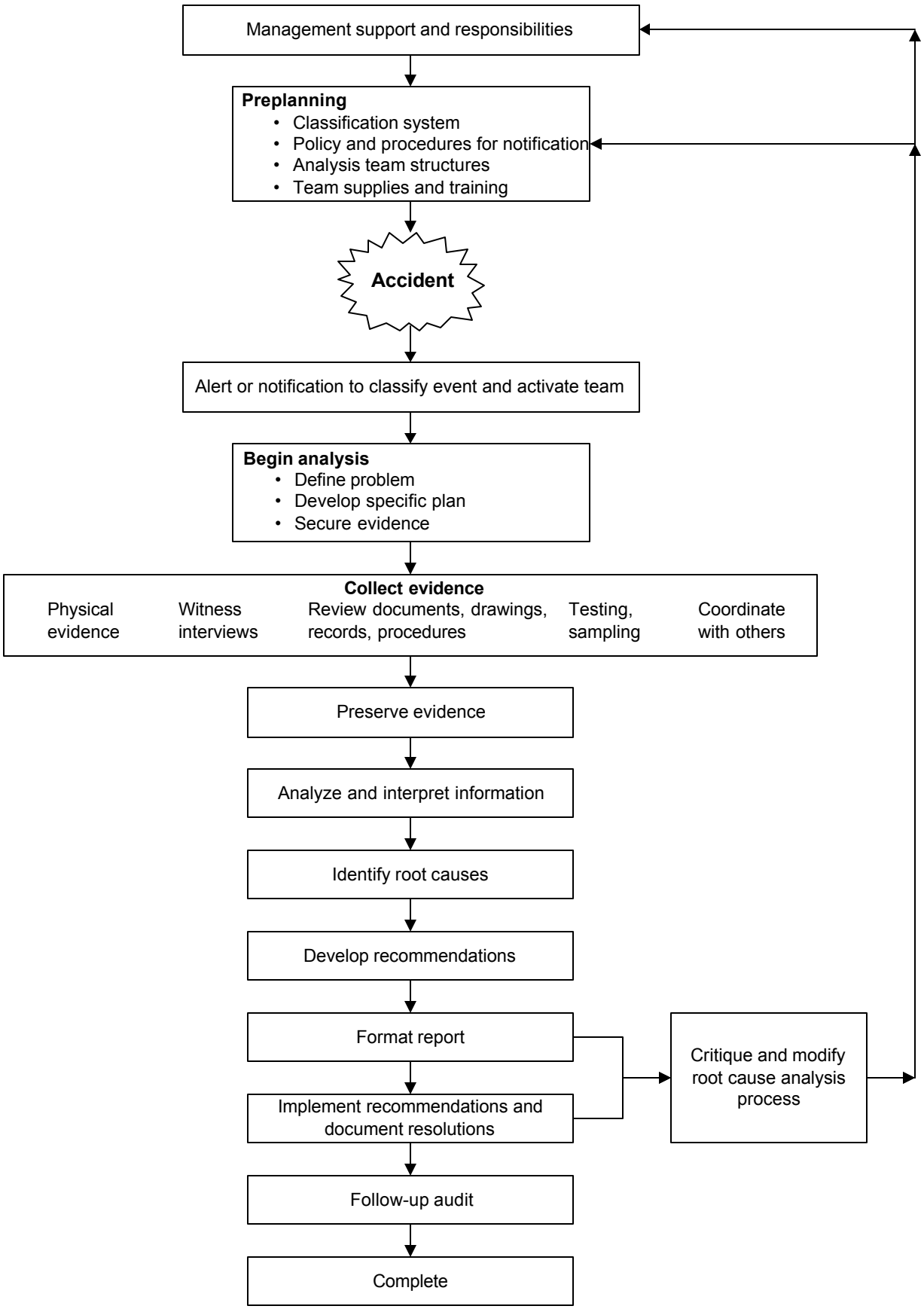
Key features of root cause analysis

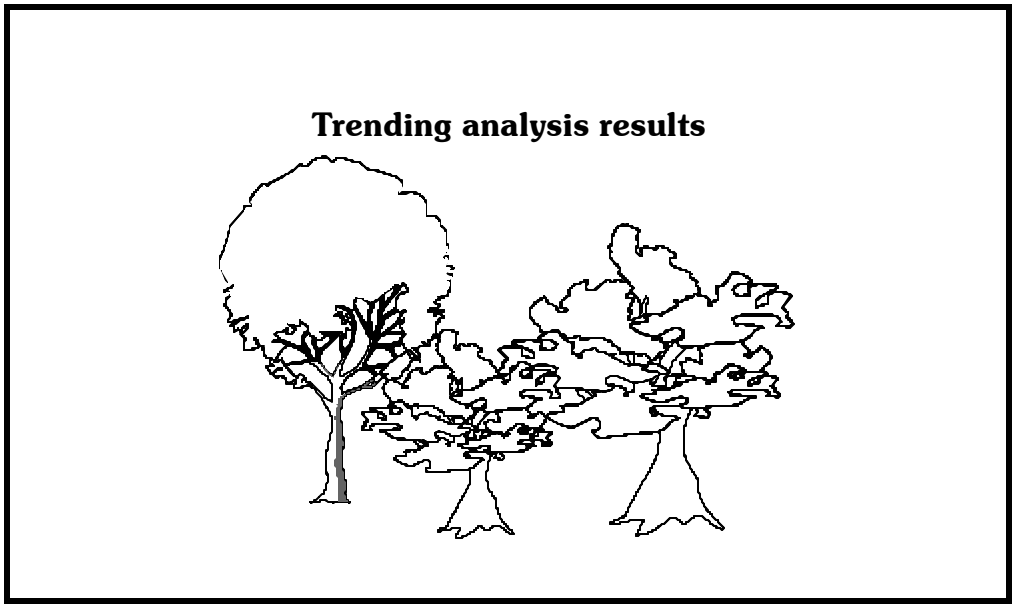
- Understanding how an accident event occurred
- Discovering the underlying root causes (management system weaknesses) of the key contributors (causal factors)
- Developing and implementing practical and effective recommendations for preventing future accidents

Key differences from traditional problem solving

- Logical reasoning through cause-effect relationships
- Rigorous focus on factual data versus supposition
- Range of possibilities considered
- Management system perspective
- Multiple root causes identified
- Systematic processes and tools make effective data trending possible

The flowchart on the following page is modeled after the American Institute of Chemical Engineers' process for conducting incident investigations. It illustrates the complete process of performing root cause analysis.


Management support and responsibilities
Preplanning
• Classification system
• Policy and procedures for notification
• Analysis team structures
• Team supplies and training
Accident
Alert or notification to classify event and activate team
Begin analysis
• Define problem
• Develop specific plan
• Secure evidence
Collect evidence
Physical evidence
Witness interviews
Review documents, drawings, records, procedures
Testing, sampling
Coordinate with others
Preserve evidence
Analyze and interpret information
Identify root causes
Develop recommendations
Format report
Implement recommendations and document resolutions
Critique and modify root cause analysis process
Follow-up audit
Complete



4.2 Trending analysis results

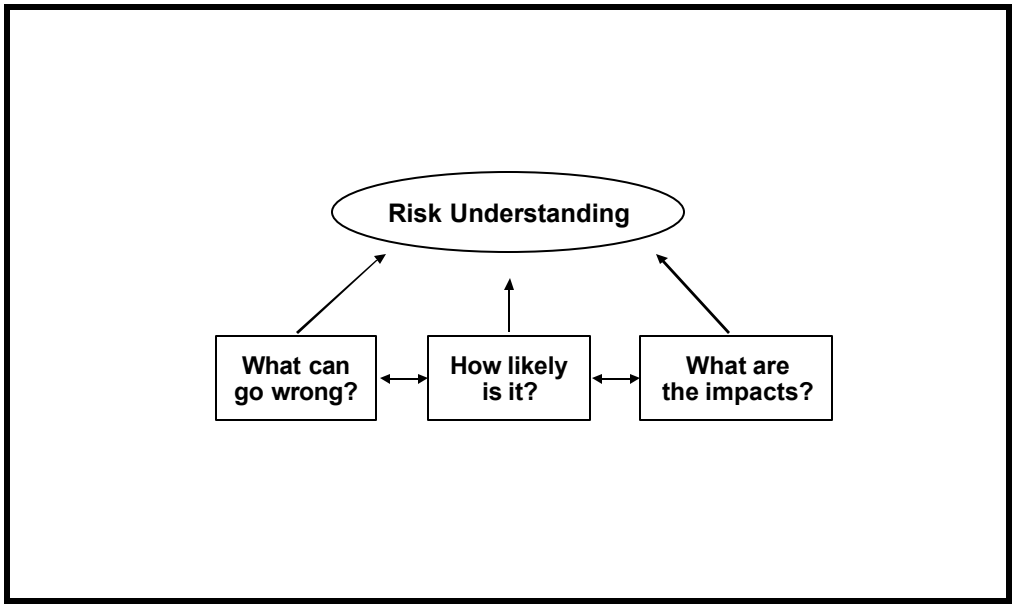
Root cause analysis results can be trended to identify persistent problem areas. Analysis teams focus on one specific event and reasonable methods for preventing recurrence. Organizations should identify systemic problems that contribute to groups of events. Trending provides the ability to associate related events.

Trending is performed by sorting various characteristics of events of interest. Trending can provide correlation of events to:

- — country of operation
- — division
- — industry sector
- — facility or vessel
- — operating areas
- — types of accidents
- — job positions
- — operating modes
- — timing (seasons, days, time of day, etc.)
- — environmental conditions
- — contributing events
- — event sequences
- — root causes

Benefits of trending

- Facilitates performance assessments and projections
- Identifies persistent management deficiencies (root causes)
- Highlights unique, unrecognized, or improperly defined risks
- Identifies misallocated management resources
- Flags sudden changes in performance, either positive or negative
- Provides correlation of changes in performance to events producing such changes
- Highlights risk assessment weaknesses



5.0 Characterizing Risk

Understanding risk requires answers to the following questions:

What can go wrong?

Risk assessment methods are used to identify combinations of events that can create marine casualties. These can include equipment failures, human errors, and external events. Based on the quantity and types of events that may occur, an analyst gains a good understanding of the risk associated with an issue of concern.

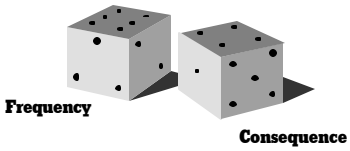
How likely is it?

Likelihood is usually expressed as the probability or frequency of an accident occurring. If the likelihood is low enough, analysts may conclude that a possible accident scenario is not credible, not of concern, or of extremely low risk. But, the criteria for making such judgments often change with the type and severity of the consequence related to the possible accident.

What are the impacts?

An accident can affect many areas of concern with different degrees of negative results. For example, a ship's boiler that is lit without proper purging can explode, causing major equipment damage and personnel injury. However, this accident may not cause environmental damage or public injury. The type and severity of consequences related to an accident help an analyst understand and judge risk.

Elements of risk



- **Risk is the combination of frequency (F) and consequence (C), often expressed as F x C**
- **Two categories of risk**
  - **risks that can be reduced or eliminated**
  - **remaining risks**

5.1 Elements of risk

Frequency. The frequency of events is often expressed as events per year. However, other bases for expressing how frequently an event will occur are also used. These include events per mile traveled, events per transit, events per ton of material moved, etc.

The frequency should be determined from past data if a large number of events have occurred. However, we usually focus on accidents with severe consequences for which few data records exist. For these events, frequency is calculated using risk assessment models.

The frequency of any event is based on (1) how often the hazard is present (i.e., how many times an operation is performed) and (2) the probability of experiencing the accident during any exposure to the hazard. Some descriptions of risk will explicitly describe frequency as the number of exposures to the hazard, multiplied by the probability of an accident during each exposure.

Consequence. Consequence is measured by the magnitude of its effects. Consequence is expressed as the number of people injured or killed, area affected, outage time, mission delay, dollars lost, etc.

Risk. The risk of a potential accident is often calculated as the combination of the frequency and consequence. This way, we can compare the risks of different operations and potential accidents. However, you should also compare the two *consequences,* because we often judge risk with a higher priority given to high-consequence events.

For example, suppose Potential Accident #1 has a frequency of once in 100 years and a consequence of $10,000. Potential Accident #2 has a frequency of once in 10,000 years and a consequence of $1 million. The risk of either potential accident is $100/yr ($10,000 x 1/100 yr or $1 million x 1/10,000 yr), but you might be more concerned about Potential Accident #2 than Potential Accident #1 based on the severity of the consequence.

Risk acceptance criteria. Any operation has risks. Once these risks are known, we can take steps to reduce them (e.g., insulate hot surfaces to reduce the chance of getting burned) or eliminate them (e.g., switching to nonflammable cleaning materials to eliminate a fire hazard). However, some known risks are accepted as the *cost of doing business*. These remaining risks, known as residual risks, should be within an organization's risk acceptance criteria.

Risk characterization methods

- **Quantitative**
  - **point risk estimate**
  - **categorization**
  - **probability distributions**
- **Qualitative**
  - **subjective prioritization**
  - **basic scenario ranking**
  - **criteria-based scenario ranking**

5.2 Risk characterization methods

Risk assessment involves processing a large quantity of data: Often hundreds or even thousands of accident scenarios must be evaluated to estimate the risk of an operation. An analyst should consider the level of detail needed in the risk results before starting the risk assessment process. Qualitative methods, as well as coarse and detailed quantitative methods, can characterize risk. Qualitative methods may suffice when focusing on the *big picture* and identifying general operations where higher risk exists. However, in other situations, a more detailed risk assessment is needed.

Quantitative risk characterization

- **Point risk estimate**
- **Categorization**
- **Probability distributions**

5.2.1 Quantitative risk characterization

Quantitative risk characterization methods provide decision makers with precise descriptions of risk; however, these methods often involve detailed studies that are very resource intensive. Also, be careful not to confuse precise descriptions of risk with the accuracy or certainty of those descriptions. Applying quantitative risk characterization methods generally requires a substantial level of experience and expertise among analysis team members. Two common forms of quantitative risk characterization are the following:

Point risk estimates. An analysis team uses historical data from directly related operational experience, expert judgment, and data published from other applications of similar equipment or human activities to estimate (1) the frequency of initiating events for various accident scenarios and (2) the probability of failure for each safeguard. The effect of the consequence, often measured in cost or injuries and deaths, is also estimated.

Categorizations. A risk assessment team assigns accident scenarios to appropriate likelihood and consequence categories. The combination of likelihood and consequence category is used to assign a risk level to the scenario.

Probability distributions. A risk assessment team assigns probability distributions to reflect the possible range of event frequencies, probabilities, and consequences that may be applicable for a specific assessment. This method is more robust than simply selecting point estimates as described above because the uncertainty associated with each key frequency, probability, or consequence number is modeled. However, this method is considerably more complicated to apply and will not be discussed further in these *Guidelines*.

Point risk estimate characterization

$$\text{Risk}_{\substack{\text{Accident}\\\text{scenario}}} = F_{\substack{\text{Accident}\\\text{scenario}}} \times C_{\substack{\text{Accident}\\\text{scenario}}}$$

Where

$$F_{\substack{\text{Accident}\\\text{scenario}}} = F_{\text{Incident}} \times P_{\substack{\text{Safeguard \#1}\\\text{being}\\\text{undependable}}} \times P_{\substack{\text{Safeguard \#2}\\\text{being}\\\text{undependable}}} \times \cdots$$

and

F = frequency of occurrence
C = consequence
P = probability of occurrence

5.2.2 Point risk estimate characterization

Point estimates of risk provide decision makers with very precise information about the absolute magnitude of risk associated with specific activities. These precise estimates are particularly useful when decisions will be sensitive to small, subtle differences in risk.

Example for oil spill scenarios

Scenarios	Incident	Failed Safeguards			Scenario Frequencies
Scenario 1	Valve leaks (1/y)	Flow not stopped (0.1)	x	Oil enters water (0.01)	= 0.001/y
Scenario 2	Hose leaks (0.1/y)	Flow not stopped (0.1)	x	Oil enters water (0.1)	= 0.001/y
Scenario 3	Hose ruptures (0.01/y)	Flow not stopped (1.0)		Oil enters water (1.0)	= 0.01/y
				$F_{accident}$	= 0.012/y

Risk = 0.012/y x $10,000 = $120/y

As you can see from the table above, three different scenarios have been identified that could cause the same accident, which has an associated consequence of $10,000. The accident frequency is the sum of the scenario frequencies. Knowing the accident frequency, consequence, and risk, management can now determine if the accident risk is acceptable. If not, these same results help us focus on areas where additional control efforts may be needed.

Limitations of point risk estimate

- Accuracy depends on accuracy and completeness of scenario models and specific likelihood and consequence data for each event
- Very resource intensive for detailed studies
- Point estimate choices are often based on subjective choices

Risk characterization using categorization

- **Can provide most types of risk-based information**
- **Generally efficient to apply**
- **Often an excellent screening approach**

5.2.3 Risk characterization using categorization

The risk assessment process changes very little if risk is to be characterized using categories instead of point estimates. In this case, the analyst must (1) define the likelihood and consequence categories to be used in evaluating accident scenario risk acceptability and (2) define the level of risk associated with each likelihood and consequence category combination. In defining categories, be careful to provide enough so that meaningful results are obtained, but not so many that risk assessment teams have difficulty assigning category values to scenarios.

For example, using too few categories may cause analysts to assign all the accident scenarios to the same risk level. In this case, very little is learned in the risk assessment process and no direction is given as to where to focus management controls. Too many categories, on the other hand, will consume excessive amounts of the risk assessment team's time in determining the *right* category assignment for each accident scenario.

Frequency and consequence categories

The following tables are the basis for a scenario-based risk categorization system. Multiple consequence classification criteria may be required to address safety, environmental, operability, and other types of consequences.

Example criteria for consequences

This table is an example of a scheme for estimating the effects of a specific accident scenario. The most applicable category would be chosen for the scenario using the definitions provided.

Example Types of Effects*				
Severity	**Safety Impact**	**Environmental Impact**	**Economic Impact**	**Mission Impact**
Major (1)	One or more deaths or permanent disability	Releases that result in long-term disruption of the ecosystem or long-term exposure to chronic health risks	≥ $3M	≥ $3M
Moderate (2)	Injury that requires hospitalization or lost work days	Releases that result in short-term disruption of the ecosystem	≥$10K and <$3M	≥$10K and <$3M
Minor (3)	Injury that requires first aid	Pollution with minimal acute environmental or public health impact	≥ $100 and <$10K	≥ $100 and <$10K

* Losses in these categories result from both immediate and long-term effects (e.g., considering both acute and chronic effects when evaluating safety and health).

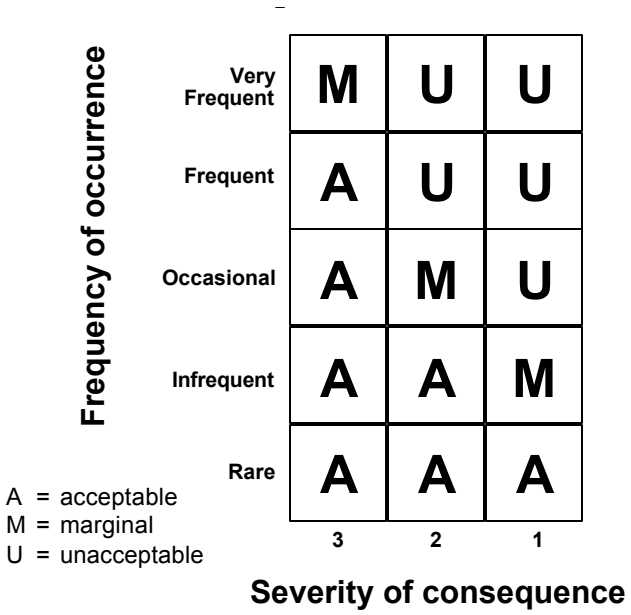
Example criteria for frequency

This table is an example of a scheme for scoring frequencies of accident scenarios. The most applicable score would be chosen for each scenario using the descriptions provided.

Frequency Category	Description
Very Frequent	**From 10 to 100 events per year in the port**
Frequent	**From 1 to 10 events per year in the port**
Occasional	**From 1 event every 10 years to 1 event per year in the port**
Infrequent	**Less than 1 event every 10 years in the port**
Rare	**Not expected to occur in the port**

Example risk matrix

The following matrix provides a mechanism for assigning risk, and making risk acceptance decisions, using a risk categorization approach. Each cell in the matrix corresponds to a specific combination of likelihood and consequence. Thus, each cell indicates the risk of a scenario having that combination of likelihood and consequence. Each cell in the matrix can be assigned a priority number or some other risk descriptor, as shown in the matrix below. An organization must define the categories it will use to score risks and, more importantly, how it will prioritize and respond to the various levels of risk associated with cells in the matrix.



Example Risk Acceptability for Oil Spills Throughout a Port

Scenario	Frequency and Severity Estimates			Risk Acceptability
	Level 3 Severity	Level 2 Severity	Level 1 Severity	
Scenario 1: Hose leak or rupture during a transfer	Very frequent (Risk: M)	Infrequent (Risk: A)	Rare (Risk: A)	M
Scenario 2: Tank rupture during a grounding	Occasional (Risk: A)	Occasional (Risk: M)	Infrequent (Risk: M)	M
Scenario 3: Tank overfill during a transfer	Frequent (Risk: A)	Infrequent (Risk: A)	Rare (Risk: A)	A

Example loss estimates

The significance of a risk matrix can be further understood by generating the estimated losses associated with it. In the table below, the risk assessment team estimated how often each scenario will occur and how often it will result in consequences in each of these severity levels. For example, the team determined that Scenario #3 will result in a Level 3 severity 1 to 10 times per year and essentially never result in a Level 1 severity. You can add the ranges of the frequency estimates for all scenarios to determine the Frequency Summary of each severity level. To get the range of Expected Losses for each severity level, multiply the upper and lower bounds of the Frequency Summary with the average consequence for the severity level. The total expected range of annual losses presented below the table is the sum of the Expected Losses for all severity levels.

Example Loss Estimates for Oil Spills Throughout a Port

Scenario	Frequency and Severity Estimates		
	3 ($100 to $10K) Average Consequence: $3K	**2** ($10K to $3M) Average Consequence: $300K	**1** (>$3M) Average Consequence: $5M
Scenario #1 **Hose leak or rupture during a transfer**	**Very Frequent** 10/yr to 100/yr	**Infrequent** 0/yr to 0.1/yr	**Rare** 0/yr
Scenario #2 **Tank damage during a grounding**	**Occasional** 0.1/yr to 1/yr	**Occasional** 0.1/yr to 1/yr	**Infrequent** 0/yr to 0.1/yr
Scenario #3 **Tank overfill during a transfer**	**Frequent** 1/yr to 10/yr	**Infrequent** 0/yr to 0.1/yr	**Rare** 0/yr
Frequency Summary (by Severity Level)	11.1/yr to 111/yr	0.1/yr to 1.2/yr	0/yr to 0.1/yr
Expected Losses (by Severity Level)	Using the Average Consequence: ~$33K/yr to $333K/yr	Using the Average Consequence: ~$30K/yr to $360K/yr	Using the Average Consequence: ~$0K/yr to $500K/yr

Total Expected Annual Losses: ~$63K/yr to ~$1.2M/yr

Limitations of risk characterization using categorization

- Less precise than point estimates
- Accuracy depends on
  - accuracy of scenario models
  - judgment and experience of those assigning scores for scenarios
  - quality of available scenario data
- Results are often subjective, especially for rare scenarios

Qualitative risk characterization

- **Subjective prioritization**
- **Basic scenario ranking**
- **Criteria-based scenario ranking**

5.2.4 Qualitative risk characterization

As you would expect, qualitative methods are easier and faster to use in characterizing risk than quantitative methods. These methods generally require less experience and expertise among risk assessment team members as well.

Subjective prioritization — A risk assessment team assigns accident scenario risk (i.e., priority) based on its collective judgment of the likelihood and severity of the failures involved in the scenario

Basic scenario ranking — A risk assessment team assigns points to each failure in a accident scenario based on the type of each failure. The points are summed to get the scenario risk. Higher scores indicate lower risks because more failures, or failures of more reliable safeguards, are required to complete the sequence.

Criteria-based scenario ranking — A risk assessment team determines if accident scenario risk is acceptable or unacceptable based on the number and type of failures described in the accident scenario. Scenarios with unacceptable risks are subject to further control measures.

Subjective prioritization

- **Identify potential accident scenarios using structured hazard assessment techniques**
- **Subjectively categorize scenarios according to their perceived level of risk**

5.2.5 Subjective prioritization

Subjective prioritization identifies potential accident scenarios using structured hazard assessment techniques. This technique subjectively assigns each scenario to a priority category based on the perceived level of risk. Priority categories can be the following:

- low, medium, high
- numerical assignments
- priority levels

Of course, the results from this technique are highly dependent on the experience of the team performing the prioritization.

Example of subjective prioritization of 20 scenarios:

- **Priority 1** ⇨ **Scenarios 3, 7, 15**
- **Priority 2** ⇨ **Scenarios 1, 5, 16, 18, 19**
- **Priority 3** ⇨ **Scenarios 2, 4, 6, 8, 9, 10, 11, 12, 13, 14, 17, 20**

Limitations of subjective prioritization

- Very subjective: Results are highly dependent on the analyst's perception of risk
- Provides only general prioritization of scenarios
- Provides limited direction to management on where to focus control efforts

Basic scenario ranking

- **Identify potential accident scenarios**
- **Score scenarios based on types and numbers of events**
- **Prioritize based on scores**

5.2.6 Basic scenario ranking

The basic scenario ranking technique allows an analyst to systematically prioritize various accident scenarios of interest. Scores are assigned to each failure in an accident scenario, and the values are totaled to yield a scenario risk score. Similarly, the risk scores for all scenarios that have the same outcome can be totaled to estimate risk. Thus, this method allows analysts to screen various types of accidents as well as scenarios that contribute to accidents.

Example

The table on the next page presents a set of accident scenarios that were evaluated using a scenario ranking methodology. The scoring guidelines used to rank these scenarios are as follows:

- 1 point for any event (operating conditions, environmental conditions, human actions, equipment actions, etc.) expected to occur regularly (EE)
- 2 points for each human error (HE)
- 3 points for each active equipment failure (AEF)
- 4 points for each infrequent external event (IEE)
- 5 points for each passive equipment failure (PEF)

Low scores indicate that the scenario is a high risk. In this method, additional safeguards that reduce risk by adding layers of protection produce larger ranking numbers.

Note that in the example below, the scenario that is ranked highest does not have the lowest score. This is because of the strong dependencies among the human errors associated with the highest-ranked scenario. Common-cause failures can be difficult to factor explicitly into qualitative risk-based schemes.

Some ranked accident scenarios for catastrophic rupture of cargo tank A

Rank	Accident Scenario	Types of Events	Score Based on Types and Numbers of Events
1*	Operator leaves valve A open, operator leaves valve B open, and operator fails to verify that valves A and B are closed before introducing hazardous material into the tank	HE, HE, HE	6
2	Major external impact	IEE	4
3	Mechanic improperly calibrates the relief valve on cargo tank A, and pressure control valve for cargo tank A sticks closed	HE, AEF	5
4	Catastrophic rupture of cargo tank A	PEF	5
5	Operator fails to open the isolation valve under the relief valve on cargo tank A after maintenance of the relief valve, operator fails to detect improperly positioned valve during monthly status checks of special valves, operator inadvertently misdirects a high-pressure feed stream into cargo tank A, and operator fails to detect and mitigate rising pressure (based on other pressure indications)	HE, HE, HE, HE	8
6	Operator fails to open the isolation valve under the relief valve on cargo tank A after maintenance of the relief valve, operator fails to detect improperly positioned valve during monthly status checks of special valves, pressure controller erroneously commands pressure control for cargo tank A to close, and operator fails to detect and mitigate rising pressure (based on other pressure indications)	HE, HE, AEF, HE	9

*This scenario is ranked as more important than three other scenarios with lower scores because the analyst identified strong dependencies among the three human errors associated with this scenario.

Limitations of basic scenario ranking

- Provides only general prioritization of scenarios
- Basis of scoring has inherent limitations and inaccuracies

Criteria-based scenario evaluation

- **Derived from the basic scenario ranking method**
- **Efficient to implement**
- **Effective screening tool**

5.2.7 Criteria-based scenario evaluation

The criteria-based ranking is a derivative of the basic scenario ranking method. The two key differences are that numerical scores are not used and the scenario risk results are binary (i.e., pass or fail). Specific recommendations are made based on failure to meet the acceptance criteria.

Preestablished criteria

Preestablished criteria are listed in the table below. The left-hand column of this table shows the type of evaluation criteria illustrated by the actual criteria in the right-hand column. The specific scenario can now be evaluated based on how well it meets these specific preestablished criteria.

Type of Criteria	Examples
Number of safeguards that must fail before a specific accident of interest occurs (i.e., the number of events in each scenario)	There may not be any one-event scenarios capable of causing a major explosion in an engine room Two safeguards must be in place to prevent a release of oil from entering the water
Types of safeguards that must fail before a specific accident of interest occurs (i.e., the types of events in each scenario)	There may not be a situation in which a high pressure excursion in a boiler could occur without at least one equipment failure in addition to the equipment failure or human error that initiated the high pressure (i.e., no complete dependence on human response to the upset condition) An active and a passive equipment protection, or two passive equipment protections, are required for any scenario capable of causing a catastrophic consequence
Combinations of the number and types of safeguards that must fail before a specific accident of interest occurs (i.e., the numbers and types of events in each scenario)	Single-event scenarios are only acceptable if the event is a passive equipment failure **and** the worst-case effect would not be catastrophic Scenarios involving multiple passive equipment failures are considered practically impossible unless there is some dependency (i.e., common cause) between the failures

Scenario evaluation

This table presents some accident scenarios evaluated against preestablished criteria. Recommendations are made when the evaluation criteria are not met.

Item	Accident Scenario	Types of Events	Acceptable?	Recommendation
1	Operator leaves valve A open, operator leaves valve B open, and operator fails to verify that valves A and B are closed before introducing hazardous material into the tank	HE, HE, HE	No	Needs equipment protection
2	Major external impact	IEE	Yes	None
3	Mechanic improperly calibrates the relief valve on cargo tank A, and pressure control valve for cargo tank A sticks closed	HE, AEF	Yes	None
4	Catastrophic rupture of cargo tank A	PEF	Yes	None
5	Operator fails to open the isolation valve under the relief valve on cargo tank A after maintenance of the relief valve, operator fails to detect improperly positioned valve during monthly status checks of special valves, operator inadvertently misdirects a high-pressure feed stream into cargo tank A, and operator fails to detect and mitigate rising pressure (based on other pressure indications)	HE, HE, HE, HE	No	Needs equipment protection
6	Operator fails to open the isolation valve under the relief valve on cargo tank A after maintenance of the relief valve, operator fails to detect improperly positioned valve during monthly status checks of special valves, pressure controller erroneously commands pressure control for cargo tank A to close, and operator fails to detect and mitigate rising pressure (based on other pressure indications)	HE, HE, AEF, HE	Yes	None

Limitations of criteria-based scenario evaluation

- Basis of criteria has inherent limitations and inaccuracies

Risk reduction methods

- **Point estimates**
- **Categorization**

5.3 Risk reduction methods

As presented earlier in this section, risk assessment involves processing a large quantity of data to characterize the risk of a system or activity. The next step is understanding what changes will reduce the risk to acceptable levels. Point estimates and categorization methods can be used to assess the impact of change.

Point estimates. Point estimates provide precise calculations of the risk associated with a particular activity. When recommending change, the same point estimate process can be applied to the activity, considering the frequency of initiating events and the failure of safeguards both before and after the proposed change. Comparing the point estimates after the change to those before provides an assessment of the impact of the change.

Categorization. Using likelihood and consequence categories, the outcomes of each applicable scenario are evaluated both before and after the change. Results are generally presented in a tabular or matrix form to provide the analyst with an overall assessment of the change for all affected scenarios.

Example risk reduction using point risk estimate

Similar to the example shown earlier in this section, a risk assessment team identified three scenarios that could cause the same accident, which has an associated consequence of $10,000. The accident frequency is the sum of the scenario frequencies.

Scenarios	Incident	Failed Safeguards			Scenario Frequencies
Scenario 1	Valve leaks (1/y)	x Flow not stopped (0.1)	x	Oil enters water (0.01)	= 0.001/y
Scenario 2	Hose leaks (0.1/y)	x Flow not stopped (0.1)	x	Oil enters water (0.1)	= 0.001/y
Scenario 3	Hose ruptures (0.01/y)	x Flow not stopped (1.0)		Oil enters water (1.0)	= 0.01/y
				$F_{accident}$	= 0.012/y

Risk = 0.012/y x $10,000 = $120/y

After evaluating the three scenarios and reviewing the equipment associated with the accidents and the safeguards, the team noted that providing greater containment capacity under the hose would add an additional barrier against oil entering the water from a hose rupture. The following table illustrates the expected risk level after implementing this modification.

Scenarios	Incident	Failed Safeguards			Scenario Frequencies
Scenario 1	Valve leaks (1/y)	x Flow not stopped (0.1)	x	Oil enters water (0.01)	= 0.001/y
Scenario 2	Hose leaks (0.1/y)	x Flow not stopped (0.1)	x	Oil enters water (0.1)	= 0.001/y
Scenario 3	Hose ruptures (0.01/y)	x Flow not stopped (1.0)		Containment not effective (0.1)	= 0.001/y
				$F_{accident}$	= 0.003/y

Risk = 0.003/y x $10,000 = $30/y

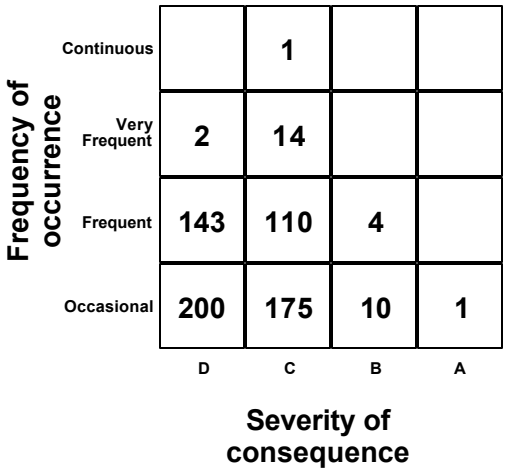
These point estimate calculations indicate a savings of $90 per year as a result of implementing this single change.

Risk Reduction = $120/y – $30/y = $90/y

Example risk reduction using categorization

Using risk categories (i.e., categories for frequency and severity) to assess change is an effective means for getting a high-level view of the overall risk associated with a system or activity and provides the analyst with a framework for recommending change. In the risk matrix below, the numbers in each box represent the number of scenarios that have the associated frequency and severity pairs. For example, when analyzing a particular vessel, the team identified 175 scenarios having an "Occasional" frequency with a "C" severity. Similarly, the team identified four scenarios having a "Frequent" frequency with a "B" severity.

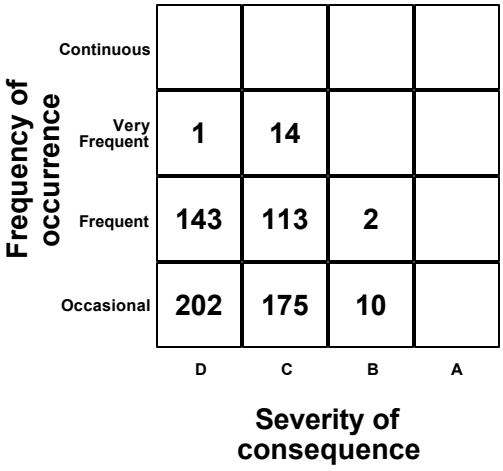
Before Implementing Changes to Reduce Risk



These types of risk matrices can be used in two ways: (1) to assess where the risks are in a system or activity and thus identify what areas should be considered for change, and (2) to illustrate the impact of change by showing how the numbers shift to other regions in the matrix.

After recommending change to a system, the team revisited the affected scenarios and reassessed the associated frequency and severity categories. The following matrix illustrates the results.

After Implementing Changes to Reduce Risk



As shown, both of the single high-risk events (i.e., the event with the high frequency and the event with the catastrophic severity) as well as some of the lower-risk issues have been reduced to lower risk categories. This revised matrix illustrates the new characterization of the risk as a result of the changes.

Once the "before" and "after" risk matrices are developed, the risk reduction impact can be determined. The following two tables show the same "before" and "after" risk matrices slightly reconfigured to aid in determining the estimated impact of the changes to the system.

Both tables summarize the frequency and severity of all loss scenarios evaluated in an analysis. For example, in the first table the team determined that there were 143 loss scenarios that could result in Level D losses 1 to 10 times per year. Next, multiply the 143 scenarios by their associated frequency range of 1/yr to 10/yr (giving 143 to 1,430 losses per year). Do the same for the rest of the scenarios under Level D and sum the results to determine the Frequency Summary of Level D losses. You can determine the Frequency Summary for the other three severity levels the same way. To get the range of Expected Losses for each severity level, multiply the upper and lower bounds of the Frequency Summary with the average consequence for the severity level. The total expected range of annual losses presented below the table is the sum of the Expected Losses for all severity levels.

Before Implementing Changes to Reduce Risk

Example Loss Estimates

Frequency	Severity Level			
	D ($1K to $10K) Average Consequence: $1K	**C** ($10K to $100K) Average Consequence: $30K	**B** ($100K to $1M) Average Consequence: $300K	**A** ($1M to $10M) Average Consequence: $3M
Continuous (Between 100 events every year and 1,000 events every year)		**1**		
Very Frequent (Between 10 events every year and 100 events every year)	**2**	**14**		
Frequent (Between 1 event every year and 10 events every year)	**143**	**110**	**4**	
Occasional (Between 1 event every 10 years and 1 event every year)	**200**	**175**	**10**	**1**
Frequency Summary (by Severity Level)	183 to 1,830 per year	367.5 to 3,675 per year	5 to 50 per year	0.1 to 1 per year
Expected Losses (by Severity Level)	Using the Average Consequence: $183K to $1.83M per year	Using the Average Consequence: $11.025M to $110.25M per year	Using the Average Consequence: $1.5M to $15M per year	Using the Average Consequence: $300K to $3M per year

Total Expected Annual Losses: $13.008M to $130.08M

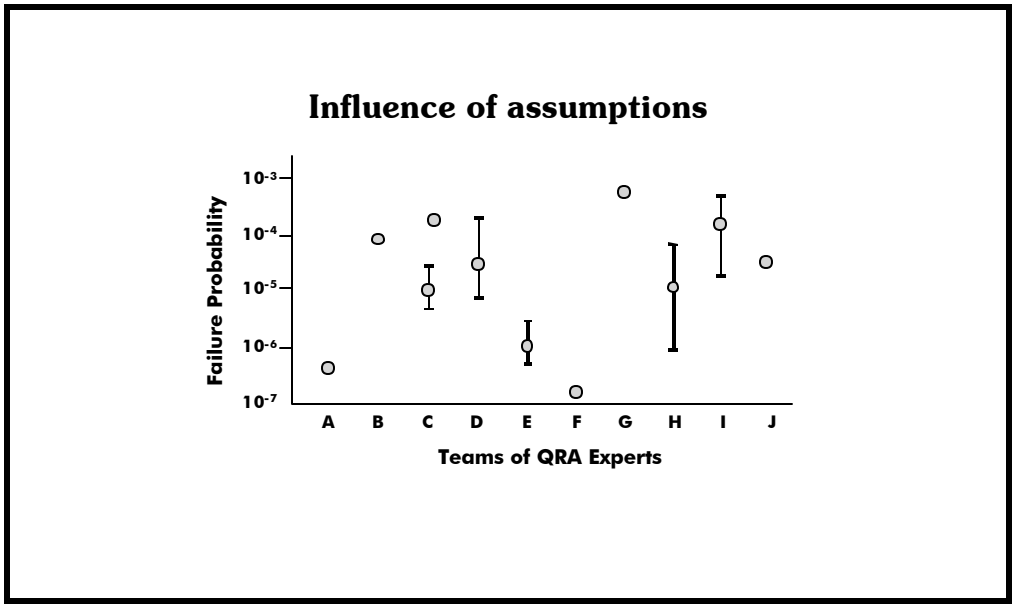
After Implementing Changes to Reduce Risk

Example Loss Estimates

Frequency	Severity Level			
	D ($1K to $10K) Average Consequence: $1K	**C** ($10K to $100K) Average Consequence: $30K	**B** ($100K to $1M) Average Consequence: $300K	**A** ($1M to $10M) Average Consequence: $3M
Continuous (Between 100 events every year and 1,000 events every year)				
Very Frequent (Between 10 events every year and 100 events every year)	**1**	**14**		
Frequent (Between 1 event every year and 10 events every year)	**143**	**113**	**2**	
Occasional (Between 1 event every 10 years and 1 event every year)	**202**	**175**	**10**	
Frequency Summary (by Severity Level)	173.2 to 1,732 per year	270.5 to 2,705 per year	3 to 30 per year	Level A losses are not expected to occur
Expected Losses (by Severity Level)	Using the Average Consequence: $173K to $1.73M per year	Using the Average Consequence: $8.115M to $81.15M per year	Using the Average Consequence: $900K to $9M per year	Level A losses are not expected to occur

Total Expected Annual Losses: $9.188M to $91.88M

The expected risk reduction after the recommended changes are made is the difference in the Total Expected Annual Losses between these two tables. In this example, the expected risk reduction is between $3.82M and $38.2M.



5.4 Influence of assumptions

When performing risk assessments, you should pay attention to any assumptions made when identifying accidents and estimating accident likelihoods and consequences. The above graph shows the results of a study in which several teams of risk experts calculated the failure probability of a system. The circles represent each team's estimated failure probability, and the bars show the uncertainty bands that some teams developed with their estimates. All the experts were given the same system design and the same failure data for the system components. The different answers were attributed to the different assumptions the experts made. When the study was repeated with the same assumptions, each team produced similar answers.

Involving the right group of stakeholders, not just one subject matter expert, and building consensus about assumptions and scope limitations will help you avoid similar problems in your own risk assessments.

Risk Assessment

Many risk assessment methods exist; however, they have common features:

- **structured**
- **predictive**
- **experience based**
- **adaptive**

6.0 Introduction to Risk Assessment Methods

There are many risk assessment methods. No one is inherently better or worse than another. They all have appropriate applications and share the following features:

Structured. Each risk assessment method has some type of structure to promote a complete examination of possible problems. Some methods have very rigid structures, while others are more flexible. More highly structured methods usually provide a more complete evaluation, but they often require much more analysis effort. Although less structured risk assessment methods require less skill to apply, they need more input from subject matter experts to make up for issues that the basic nature of the assessment might overlook.

Predictive. Some risk assessment methods can be valuable for investigating accidents that do occur. However, the main use of such methods is to characterize the possibility of future accidents. Therefore, risk assessment forecasts what is expected in the future.

Experience based. Risk assessments are predictive, but they do not ignore the past. Some of the best insight into possible accidents is based on information about the types, frequencies, and severities of past accidents in the same or similar operations. Risk assessments use this information, as well as information about corrective actions taken to address past accidents, to examine expected performance. Risk assessment methods gather this information from many sources, including records (equipment files, maintenance records, electronic databases, manufacturer information, etc.) and the opinions of subject matter experts (experienced engineers, operators, technicians, and others).

Adaptive. Most risk assessment methods can be used at various levels of detail and for many types of systems and processes. This adaptive nature makes most risk assessment methods very flexible.

Information available from risk assessments

- **Qualitative accident scenario descriptions**
- **Qualitative judgments about expected accidents**
- **Quantitative measures of factors related to loss prevention**
- **Importance of accident contributors**
- **Recommendations for improvement**

6.1 Information available from risk assessments

The information produced from risk assessments can be divided into the following categories:

Qualitative accident scenario descriptions. These descriptions define sequences of events capable of producing accidents of interest. The sequences can include equipment failures, human errors, and external influences.

Example:

- Carpenter or painter fails to wear appropriate eye protection and is injured from flying debris.

Qualitative judgments about expected accidents. Analysts often have informed opinions about whether the threat of possible accidents will exceed stated or implied loss prevention goals. These judgments are usually based on the numbers and types of events possibly leading to accidents. Judgments regarding the numbers of events would look at such things as single failures or errors versus multiple-event scenarios. Judgments regarding types of events would look at such things as equipment failures while in service, equipment failures in stand-by safety systems, mistakes made by forgetting to do something, mistakes made by doing the wrong thing, etc. These judgments are often made based on decisions made in other studies.

Example:

- The frequency and severity of injuries from personnel coming into contact with flying debris in the buoy maintenance facility will be much less when personnel are required to wear safety glasses.

Quantitative measures of factors related to loss prevention. These numeric estimates of loss prevention-related factors include measures such as reliability, availability, environmental risk, personnel or public risk, economic risk, etc. The measures are used to judge whether the threat of possible accidents exceeds numerical loss prevention goals. Sometimes these measures include studies (*what-if* scenarios) of sensitivity to changes such as implementation of recommendations, changes in operating conditions or strategies, etc.

Example:

- We expect that between one and 10 people will sustain temporarily disabling injuries leading to four or more days of lost time per person each year.

Importance of accident contributors. These results show the most important possible accidents based upon the likelihood and consequences of those accidents. Importance rankings can prioritize not only types of accidents, but also specific equipment failures and human errors.

Example:

- Failure to wear safety glasses and other personal protective equipment contributes to personnel injury at shore facilities in 50% of the identified accidents. Excessive lifting contributes to personnel injury in 35% of the accidents. The top contributors associated with the remaining 15% of the accidents are evenly divided between crew fatigue and automobile accidents.

Recommendations for improvement. Typical risk assessment results also include suggestions for reducing the frequency of accidents or preventing them altogether. These recommendations include suggestions for new or improved engineered systems, programs, policies, and items for further study. These recommendations may lessen the likelihood or consequences of an accident.

Example:

- Consider requiring personnel to wear hearing protection while using power tools such as saws and sanders. Consider enrolling these people in the formal hearing conservation program.

Life cycle approach to performing risk assessments

- **Research**
- **Design**
  - **conceptual**
  - **preliminary**
  - **detailed**
- **Fabrication/ construction/ manufacturing**
- **Operation**
  - **startup**
  - **ongoing**
- **Decommissioning**

6.2 Life cycle approach to performing risk assessments

Risk assessments can be used at every step in the life cycle of a marine system or process. The following sections discuss the use of risk assessment throughout a life cycle.

Research. Risk assessment focus at this stage is on identifying the safety and reliability of certain technologies. Assessments are performed using technical models to help us understand how failures occur over time.

Design. Risk assessment focus at this stage is on making sure that the selected operating strategy will meet overall goals. Risk managers are very interested in identifying *weak links* and opportunities for improvement in components and systems.

- **Conceptual phase.** Risk assessment focus at this stage is on deciding how overall goals can be used to define goals for individual systems. Without reviewing a lot of detail, assessments consider whether or not the system will be able to perform as expected and what changes or improvements would be needed to meet overall goals. Risk managers compare different design ideas to decide which options make the most sense based on several factors, including project risk and expected life cycle costs such as the cost of accidents and their prevention.
- **Preliminary phase.** Risk assessment focus at this stage is on how individual system goals can be used to define component goals. Assessments consider at a more detailed level whether or not the system will be able to perform as expected and what changes or improvements would be needed to meet system goals. The most favorable system performance features are based on a number of factors, including costs, loss of commerce, risk, etc.

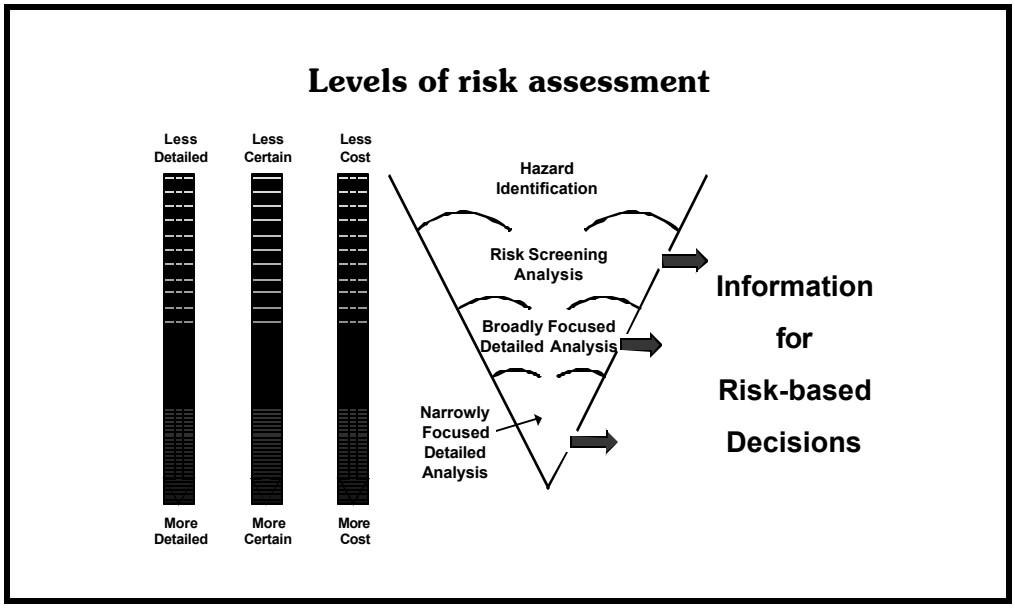
- **Detailed phase.** Risk assessment focus at this stage is on making sure the selected components work together so that the systems can meet individual component goals. Assessments consider at a component level whether or not the components will be able to perform as expected and what changes or improvements would be needed to meet component goals. The most effective component selection is based on a number of factors, including costs, loss of commerce, risk, etc. Risk managers are also interested in the following:
  - critical limits for safe and reliable fabrication, construction, and manufacturing
  - important operating limits and startup guidelines
  - appropriate preventive or predictive maintenance jobs
  - necessary spare parts and materials stores

Fabrication, construction, and manufacturing. Risk assessment focus at this stage is on making sure that specifications have been met. The assessment also tries to find any fabrication, construction, and manufacturing issues that could negatively affect the system, leading to loss. Assessments consider the importance of any identified field defects, as well as any suggested changes during fabrication, construction, and manufacturing.

Operation. Risk assessment focus at this stage is on the effectiveness of operating, maintenance, and supply strategies for reaching loss prevention goals.

- **Startup.** Risk assessment focus at this stage is on making sure that operating and maintenance plans (including programs, procedures, and training) help to achieve the safety and reliability designed into the system and are effective based on factors including costs, loss of mission, risk, etc.
- **Ongoing.** Analysis focus at this stage is on ensuring the following:
  - changes (planned, unplanned, and unintentional) do not greatly affect loss prevention performance
  - operating and maintenance plans are effective based on several factors, including costs, loss of commerce, risk, etc.

Decommissioning. Risk assessment focus at this stage is on liability issues related to removing equipment from service and what actions to take to make sure those risks stay at acceptable levels. These liability issues include safety, health, and environmental risks.



6.3 Levels of risk assessment

The goal of any risk assessment is to provide information that helps stakeholders make better decisions whenever the possibility of accidents exists. Therefore, the whole process of performing a risk assessment should focus on providing the type of risk information decision makers will need. The required types of information vary according to the following:

- The types of issues being studied
- The different stakeholders involved
- The significance of the risks
- The costs required to control the risks
- The availability of information and data related to the issue being assessed

Information needs determine how the risk assessment should be performed.

The goal is to perform the least amount of risk assessment necessary to provide information that is *barely adequate* for decision making. In other words, do as little as possible to provide the information decision makers need. Although it is not always obvious in the beginning, decision makers can often make decisions using information that has very little detail or may be uncertain. In other cases, more complicated risk assessment information is necessary. The key is always to begin risk assessments at as general a level as possible and do more detailed studies only in areas where the additional risk assessment will help the decision maker. Unnecessary risk assessment doesn't benefit the decision maker. It also uses up time and money that could have been spent solving the problem or looking at other issues.

The figure on the previous page illustrates the idea of performing different levels of risk assessment. Each level can provide more detailed and better information, but the time, money, and energy required increases at each level. The filtering effect of each level allows only the most important issues to move into the next, more detailed, level of assessment. At any point, if enough information for decision making is gathered, then the risk assessment may end at that level. Not all levels of assessment will be performed for every issue that arises. In fact, most issues will probably be resolved through risk screening or broadly focused, detailed assessments.

At each level, the risk assessment may involve qualitative or quantitative risk characterizations. The following sections briefly describe each level of risk assessment.

Hazard identification. Hazards must be understood because they are the starting point for chains of events that lead to accidents. Although hazard identification doesn't usually provide information for decision making, it is an important step. Sometimes hazard identification is specifically performed using structured techniques. Other times, usually when the hazards of interest are well known, such structured techniques are not necessary. Overall, hazard identification focuses a risk assessment on hazards of interest and the types of accidents these hazards may create.

All risk assessments begin at this level. Analysts with little risk assessment experience and some training can successfully perform these types of risk assessments.

Risk screening assessment. In most situations, there are hundreds or even thousands of ways that accidents can occur. It is usually impractical to assess each of these possibilities in detail. Risk screening assessments are very general assessments that broadly describe risk and identify the most important areas for further investigation. Sometimes this level of assessment is enough to provide all of the information decision makers need; however, more detailed assessment of important issues is most common.

Once the hazards are understood, all risk assessments should begin at this level. Generally, analysts with fairly modest risk assessment experience and some training can successfully perform these types of assessments.

Broadly focused, detailed assessment. When specific activities or systems are found to have important or uncertain risks, broadly focused, detailed assessments are generally used. These assessments use structured tools for finding specific combinations of human errors, equipment failures, and external events that lead to consequences of interest. These assessments may also use qualitative or quantitative risk characterizations so that good risk management strategies can be defined.

Most risk assessments are broadly focused, detailed assessments that use qualitative risk characterizations or, at most, quantitative categorization. These risk assessments require analysts with training and experience. This is the most advanced level of assessment that someone without a specialty in risk assessment should try.

Narrowly focused, detailed analysis. When specific human errors, equipment failures, or external events are particularly important or uncertain, more narrowly focused, detailed risk assessments are needed. These assessments generally study specific issues in great detail, often involving many numeric calculations to describe the risk.

This level of assessment should be used only for those applications truly needing this level of information. Only analysts with special training and some supervised experience should try this level of risk assessment.

The following page shows a table listing the risk assessment methods discussed in this publication. The table indicates the levels of analysis for which each method is most often used.

Risk Assessment Method	Applicability to Various Levels of Risk Assessment			
	Hazard Identification	Risk Screening	Broadly Focused, Detailed Analysis	Narrowly Focused, Detailed Analysis
Pareto analysis		X		
Checklist analysis	X	X	X	X
Relative ranking/risk indexing		X	X	
Preliminary risk analysis (PrRA)		X		
Change analysis	X	X	X	X
What-if analysis	X	X	X	X
Failure modes and effects analysis (FMEA)			X	X
Hazard and operability (HAZOP) analysis			X	
Fault tree analysis (FTA)			X	X
Event tree analysis (ETA)		X	X	X
Event and causal factor charting				X
Preliminary hazard analysis (PrHA)	X	X		